

Outlook Digitalisation 2030



**freedom
lab** thinktank for
future scenarios

Table of contents

1	Introduction
2	The digital transition
3	The digital Stack in 2030
4	Trends and development paths
5	Impact of digitalisation
6	Scenarios for the future
7	Final remarks



Abstract

The digital transition is unfolding at a high pace. Technological, economic and societal developments are occurring in rapid succession and together give shape to our digital future. Consequently, it is vital for government and society to gain perspective on possible developments, prepare themselves for the future and, where necessary and possible, redirect developments.

In view of this, the government has ordered a study into the most important trends and developments leading up to 2030. Based on eleven trends, Outlook Digitalisation 2030 paints a picture of our digital future. The study thus aims to provide an overview of the main opportunities and risks of digitalisation, but also to bring to light critical uncertainties and questions. The full report can be found in the attachment, and a succinct account of the most important findings is given below.

Most important trends

In the study, eleven dominant trends are identified. They spring from technological developments in and between different layers of the so-called digital "Stack". The Stack describes digital technology as a layered system of modular components; from raw materials to digital services, new cultural collectives and innovative models of governance. This approach enables us to think systemically about digital innovation, what role scale and network effects play in it, and the transgressive nature of digital technology.

Besides technological innovation, the trends are the consequence of societal developments as well. With every trend, there are various societal forces at play that either accelerate or slow down the trend, but also give it shape and direction. Based on a review of the literature and interviews with experts within and outside the Dutch government, the following trends are identified:

1. Mega-ecosystems: Different services are integrated into a single "super-app" that gives users direct access to, for instance, mobility, entertainment or insurances. This integration results in an optimal user experience and also creates opportunities for sustainable revenue models, such as mobility-as-a-service. This does, however, threaten the Dutch earning capacity, as it subordinates service providers to the platform. Furthermore, it gives rise to risks concerning privacy and the autonomy of citizens.

2. Decentralisation: Growing resistance to the power of large tech companies is paving the way for radical alternatives to the current internet with its winner-takes-all dynamic. Based on new design principles in which institutional innovation is embedded in technology, decentral solutions are emerging with regard to data storage, intelligence and applications.

3. Data sovereignty: The increasing importance of data to economic and societal goals is making us reconsider the value and accessibility of data. Citizens, companies and governments are obtaining data sovereignty and are enabled to make deliberate choices respecting information that's available to others.

4. Digital currencies: Cryptocurrencies could potentially enable transactions without the mediation of banks at very low cost. This is giving rise to new revenue models and remuneration structures. At the same time, cryptocurrencies could disrupt financial markets and are threatening to sideline existing players and watchdogs.

5. Compelling data: Smart cities, houses and factories generate a stream of data. Aided by artificial intelligence, this data will make our living environment increasingly predictable and more easily governed. This development raises questions with respect to the "power" of data and the limitations of technological solutions.

6. Autonomisation: In the coming years, artificial intelligence will increasingly come to act independently. At first, this will be limited to "innocuous" applications, but more complex tasks will gradually be added, and the technology will pervade our lives more deeply. However, it is still unclear whether and if so, how, we will be able to live alongside these machines and where we will draw the line as regards their responsibilities.

7. Swarm culture: Digital platforms bring people together, introduce new forms of collaboration and thus contribute to the rise and spread of new ideas. This dynamic will accelerate in the coming years, among other factors because of the advent of new interfaces, such as augmented reality that adds a digital layer to our physical reality, and low-threshold applications of artificial intelligence (e.g. deep fakes).

8. Virtual living environments: New generations of social media and games are creating virtual worlds, where users have meaningful experiences and develop new practices. Entertainment, work and education are thus shifting to the digital realm. This means that an even bigger part of our lives will take place beyond the reach of governments and digital platforms will become even more powerful.

9. Optimisation of humans: Intimate technology is helping us to overcome our physical and cognitive limitations. New interfaces are ancillary to our senses, robotics strengthen us physically and we perceive our dealings with digital assistants to be an extension of our cognitive capacities.

10. The battle of the Stacks: Superpowers are developing their own Stacks and attempting to make them the global standard. This is not merely a battle for economic and international power, but also a battle of ideas about the way we organise our society and the role we assign technology in this.

11. Vulnerability: The digital transition is making us increasingly dependent on technological systems and their developers. As a result, society and the economy are vulnerable in trade conflicts, but also to cyber espionage, sabotage and terrorism. A seemingly insignificant event such as a hack or programming error could have dire consequences.

Possible scenarios for the future

No unambiguous image emerges from the trends described and the analysis of the possible consequences of digitalisation. The trends differ too much for that and every trend is subject to many uncertainties and several divergent development paths are conceivable. Nevertheless, the different trends do bring to light what opportunities and threats could present themselves regarding the Dutch earning capacity, public administration, comprehensive wellbeing, public values and our security.

Based on the trends and underlying uncertainties, the researchers formulate four different scenarios for our digital future. In these scenarios, two questions are paramount: Which actors are leading in the digital transition and what is the purpose of the process of digitalisation? The first question specifically aligns with concerns prevalent today in respect to our dependency on a small number of (non-Dutch and non-European) companies that increasingly determine the rules of play in the digital transition.

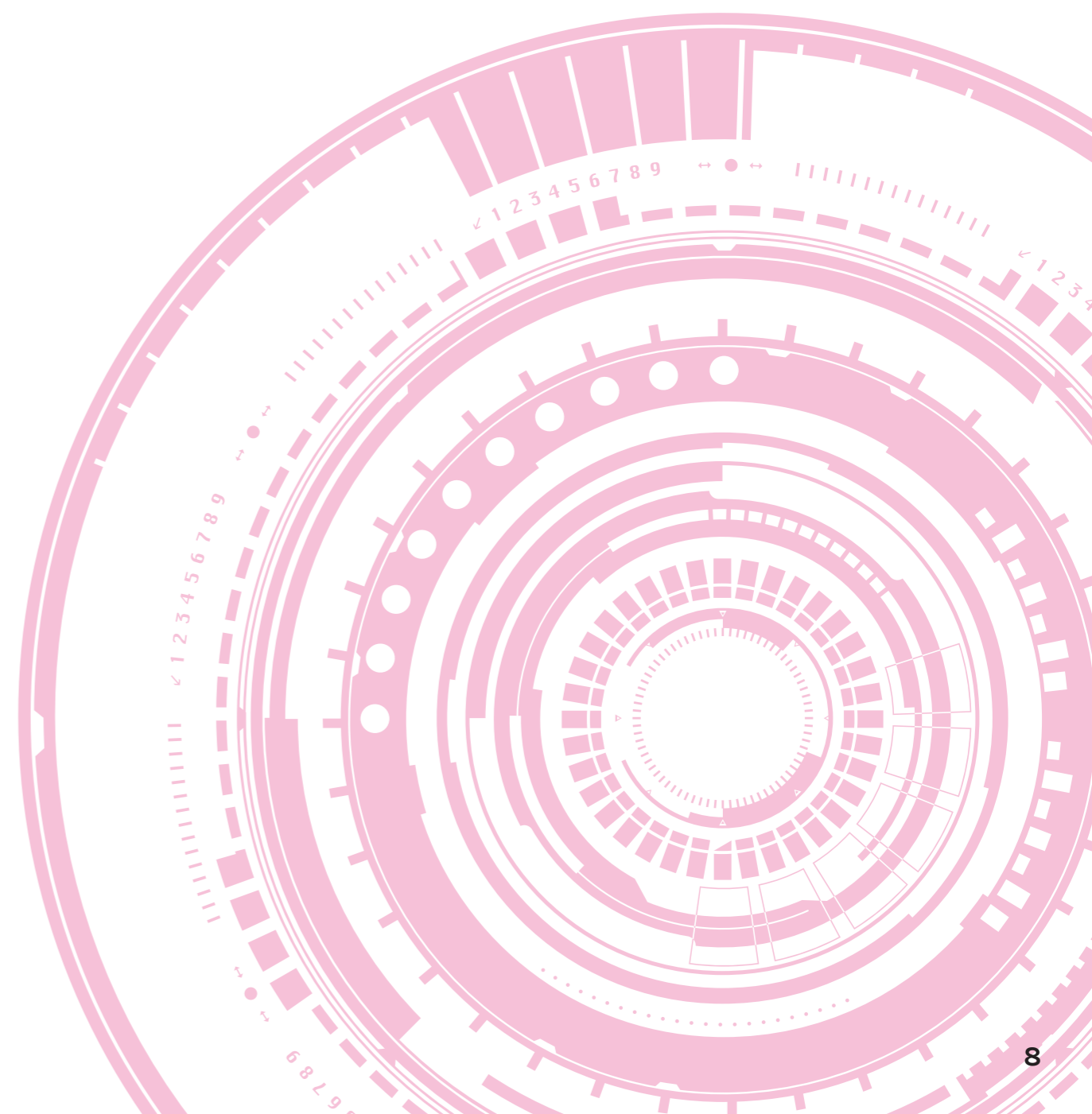
The second question is closely linked to this and pertains to the role of digitalisation in furthering equal opportunity and sustainability. Therefore, in the scenarios, the most important infrastructure and platforms remain in the hands of private parties or in fact become (semi) publicly governed, and digitalisation contributes first and foremost to economic growth or, conversely, to comprehensive well-being. These scenarios are as follows:

Acceleration: The digital infrastructure and predominant platforms are still in the hands of the large international tech companies, but the sector has shown self-correcting ability. Pressured by employees, service providers and users alike, they have become more reticent when it comes to gathering data and more transparent regarding algorithms. They have thus managed to stay ahead of the call for stricter regulation and prevent the alternative platforms, which are based on cooperation, from infringing on their position.

Conditional growth: The internet as an unregulated free state ceases to exist. It did not work for its users, had negative effects on society and compromised the Dutch and European earning capacity. Europe has therefore proceeded to implement more stringent regulation in regard to online activities and the platforms on which they occur. These regulations pertain to the handling of data and the use of algorithms, but also specifically to the impact of digitalisation on our living environment and ourselves. European companies are thriving on this internet and are gaining ground elsewhere in the world.

Radical markets: It was the market that produced the tech giants and it is the market that seems to be dismantling them. Whereas the rise of cryptocurrencies was initially seen as a speculative bubble, in hindsight, it can be said to have been a public capital injection to develop a new Stack, also known as web 3.0. An open-source infrastructure facilitates all kinds of functions, such as financial transactions and data management, without the mediation of central parties. Many of the principles of web 3.0 appear to be in alignment with the new European initiatives for a common digital market.

Responsible together: The hope that the digital transition would automatically lead to societal progress and better comprehensive well-being, has given way to the realisation that society must actively give shape to its digital future. To this aim, forms of public-private collaboration are arising in which technological innovation goes hand in hand with social, economic and institutional innovation. Openness and transparency, moreover, allow for the public-private initiatives and their solutions to be scaled up more quickly (internationally).



Chapter

1



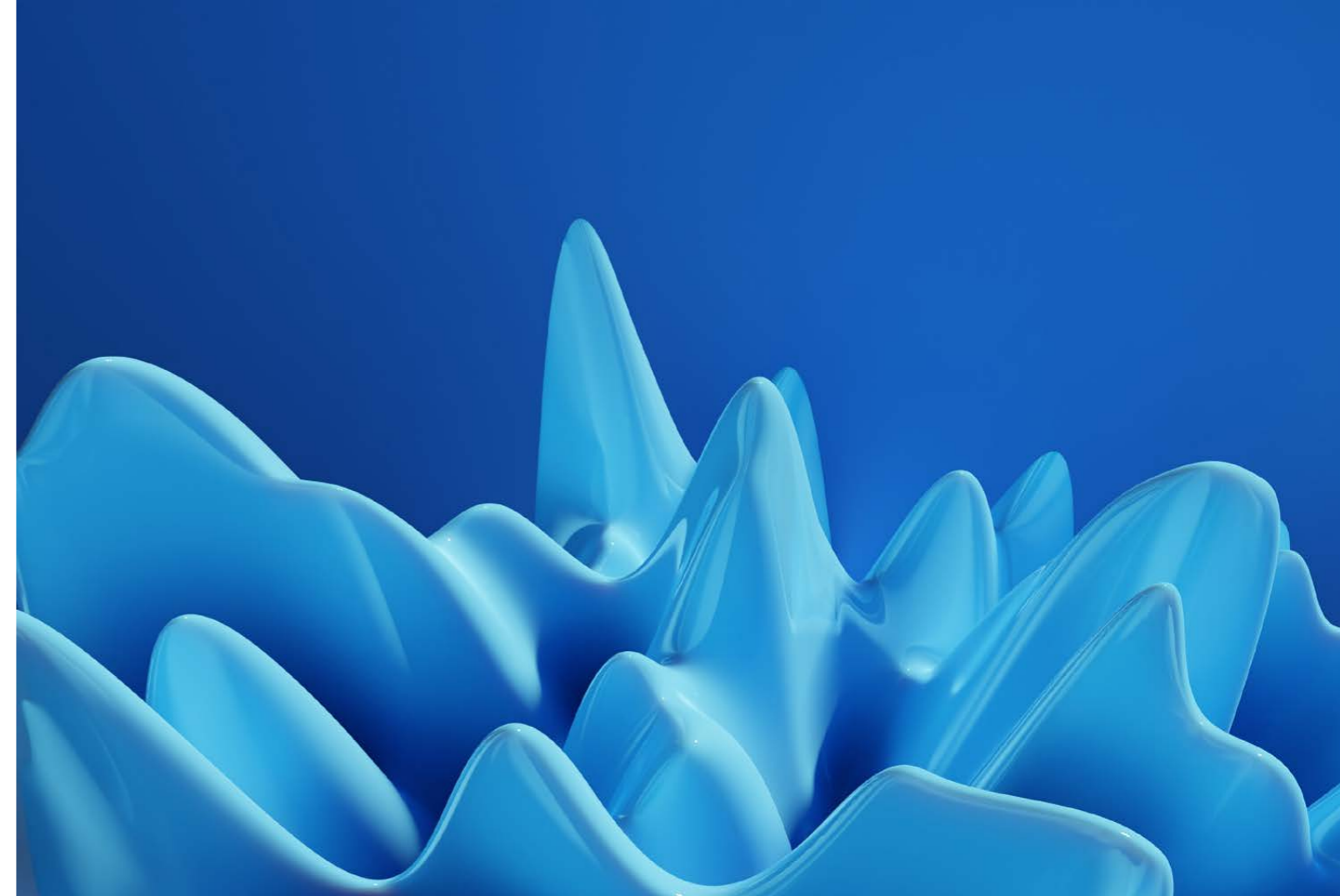
Introduction

The past has shown that every technological revolution ineluctably leads to a paradigm shift; in the economy, our daily lives and public administration. The digital transition is no exception to that. It is been underway for decades, but that does not mean the proverbial end is in sight. New technological developments and societal movements are proceeding at an unabated pace, and, considering the characteristically exponential development of digital technology, we should be prepared for an even higher pace of change.

That we are in the midst of this transition also means we can look back as well as look forward. In the first decades of this transition, we mainly embraced technology and were full of hope that it would mostly be a boon. In the past years, this has changed and the societal debate has centred expressly on the disadvantages and risks of digitalisation, such as the role of algorithms in the spread of fake news. Of course, this does not amount to a blanket rejection of technology, but we have gained better insight into the benefits and drawbacks and are better able to weigh them against each other. We see the opportunities and the necessity of fully utilising them, but are also concerned about the economic, societal and ecological consequences and the safety risks linked to this transition.

In this outlook, we provide an overview of the most important trends within the digital transition and make sense of it in relation to several different societal issues. With 2030 on the horizon, this outlook expressly looks further into the future than the Dutch Digitalisation Strategy and is largely ahead of the societal and political debate of today. By looking further into the future, asking the right questions and exposing critical uncertainties, we hope to contribute to a more fundamental debate on what goals we aspire to as a society, given the new technological possibilities ahead of us. Will we utilise them mostly to, within the existing frameworks, work, consume and exercise more intelligently and efficiently? Or will we seize these means to consider new economic principles, new forms of decision-making and new ways of living together? In other words: Are we prepared, and able, to actively and deliberately give shape to the digital transition and the paradigm shift in which it will result? Tied in with that is the question what role will be played in this by private and public parties, Dutch, European or foreign companies and users of digital systems.

In this outlook, we do not pretend to have the answers to these questions; that, after all, will be up to society. But we do offer the tools to consider possible developments, what these developments will mean to our society, and how we should deal with that. This is done by exploring eleven trends within the digital transition, in which technological developments converge with societal movements.



Technological innovation and society

New technology creates the possibility to change and improve existing practices, no matter how. This, however, does not mean that technological innovation alone determines our future. Society also makes choices in this respect; by either embracing or rejecting technology, and especially by employing it a certain way, by setting conditions and partly shaping it. The mutual influence of technology and society is a continual process of experimenting and learning, in which conscious and unconscious choices are made on either side. We cannot, in fact, infer from this that technology is "merely" a neutral tool with which society can do (or not do) whatever it pleases. Sometimes the design of technology prescribes certain ways of use, while society has never given this much thought or made any choices to this effect. Repairing any structural flaws later will generally remain impossible and it is likely that society will adjust its norms and values accordingly and accept the "new normal".

In an outlook on digitalisation, this complex dynamic means we should pay attention to both the new technologies, and the rules they prescribe, as well as the societal forces that interact with them and either welcome or possibly reject the accompanying rules of play.



Reading guide

Before we look ahead, we will first explain how digital technology and the process of digitalisation are best understood. We approach this as a layered system, the Stack, of "building blocks" that are continually connected. We illustrate the notion of the Stack by means of a historical overview of the digital transition so far. In part 3, we will discuss the most important technological developments, per layer of the Stack, which should paint a picture of what to expect in the coming decade. A more detailed description of the different sharing technologies is included as technological "Deep Dive" at the end of this document.

Based on these developments, we identify the eleven trends in part 4. Some of these trends have already been underway for several years but are likely to lead to more radical change in the coming years. Other trends are entirely new developments, of which the first signs are just now emerging. With every trend, several different societal forces are at play that either accelerate it or slow it down, but that also give shape and direction to the eventual realisation of the trend. In each description of a trend, we discuss which forces are at play, such as a movement countering the power of large technology companies or geopolitical interests. But, more importantly, each time, we outline two divergent development paths that lead to different outcomes, depending on which forces will ultimately prove the strongest.

In part 5, we then pose the question what impact the sum of these trends could have on a number of major policy themes, such as the earning capacity of the Dutch economy, our security and our comprehensive wellbeing. In part 6, we develop four different scenarios of the future in which we translate the insights from this outlook, as well as the critical uncertainties, into visions of our digital future in which several different parties are dominant and technology is utilised to achieve various societal goals.

Approach of the study

This study is based on a combination of literature review and expert interviews. Among the interviewed experts are both technologists as well as experts that regard the development and embedding of new technology from a societal or philosophical perspective. Based on these sources and interviews, we have formulated a first selection of technological building blocks and trends within the digital transition.

The building blocks are further explicated in the appendix of this document. Subsequently, the trends derived from them were tested in four working sessions with a large number of policy advisors from various ministries. In these discussions, the emphasis was on placing the trends in the context of several different policy themes. From the outcomes, we distilled the specific trends and thematic reflections of part 5. Finally, by means of a scenario exercise, together with policy advisors, we developed the four scenarios of the digital transition in 2030.

Chapter

2



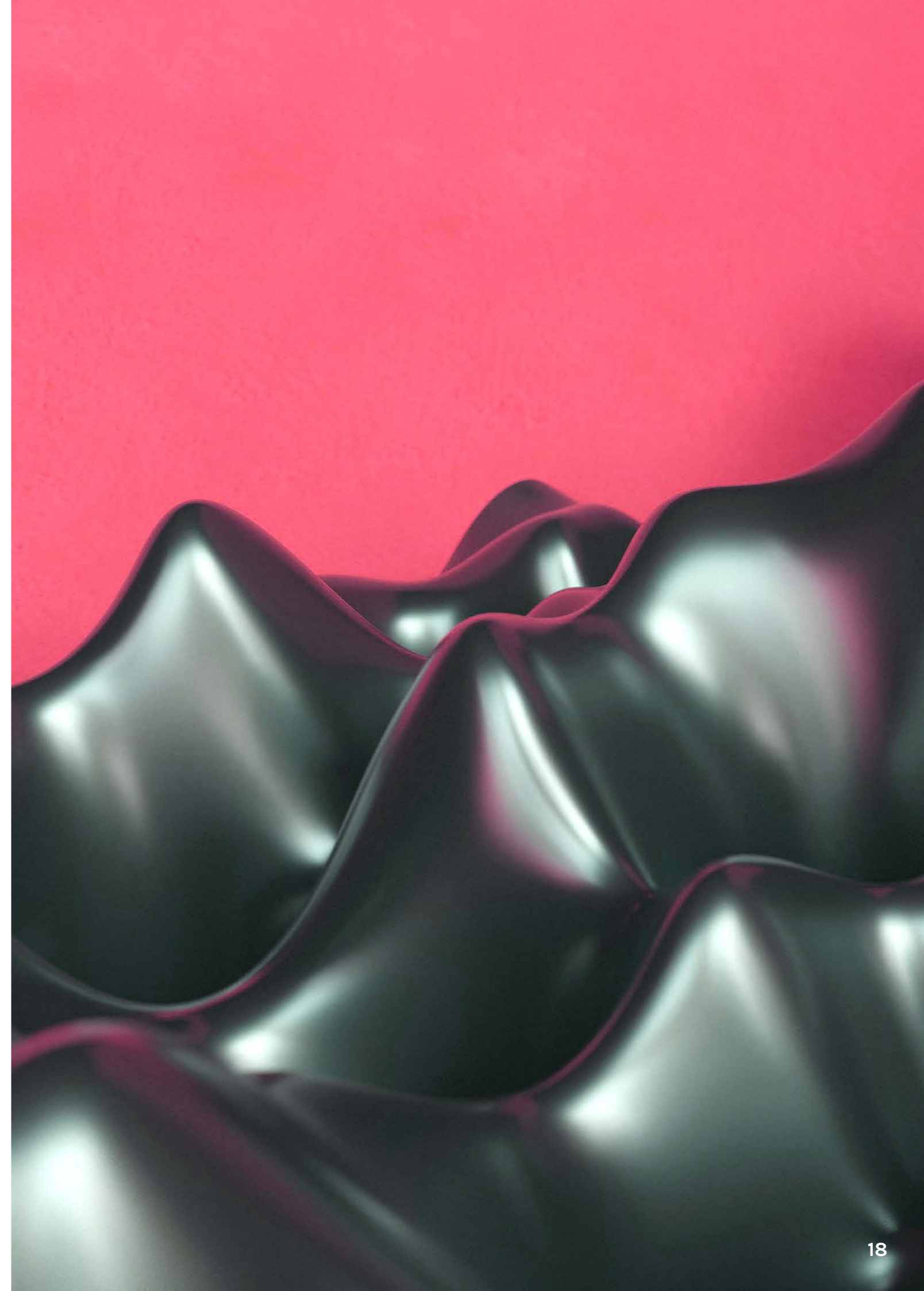
The digital transition

In many ways, the digital revolution is comparable to technological revolutions from the past, but it is also vitally different. This stems from the fact that data and software can be endlessly copied and spread at extremely low cost. Information, such as news or music, can thus be freely shared across the entire world and applications can quickly obtain a multitude of users. While a car-maker in the early 20th century was forced to make a huge investment in order to produce a small number of cars, a smart programmer can design an app for a taxi service from an attic, and almost immediately make it available to drivers and customers worldwide.

The fact that it is all about information is also visible in the architecture of digital technology. This consists of different layers between which information is continually exchanged. That is, a digital application is composed of various components that are mutually interchangeable; an app works on a phone, which consists of various components, from processor to touchscreen, and which is connected to a network. Through this network, the application communicates mainly with a server that has data and computing power.

This stratification ensures that digital solutions are easily scalable and that network effects arise when multiple users use the same service. It also means that a digital application is not necessarily bound to a single device or location. Continuous updates ensure that existing hardware keeps gaining new functions, as exemplified by Tesla cars "suddenly" being able to drive autonomously after an update, but also that we are able to use applications that run on a server in China.

If we want to understand the digital transition, we need to take account of this layered structure. Firstly, because various developments are separately taking place on the different layers. A number of these developments, such as 5G, quantum computing or artificial intelligence, will in themselves bring about great changes in the digital landscape. But, more so than of the individual building blocks, the real, paradigmatic change will be the product of the interplay between these building blocks. This raises the question: What will happen when, at a certain moment, different innovations come together and enable essentially new applications?





Digital technology as layered Stack

To clearly outline digital developments and their societal impact, it is necessary to develop a better understanding of the different technologies at play and their interdependence. To this aim, in this report we use the framework of the Stack. This helps us to dissect each digital system, be it a smartphone, a cloud platform or the entire Internet, with a fixed number of subcategories of technologies.

The thinking in terms of vertically stacked technology layers originates in software development. According to the principle of "separation of concerns", elements are delineated based on their function and internal coherence, which leads to a high degree of modularity, which thus characterises digital systems. That is, the lower layers generally refer to more stable infrastructural technologies, while the higher layers refer to more user and context specific infrastructural combinations that consequently are more fluid and adaptive.

However, whereas developers apply this to build digital systems, we will employ it to systematically consider the impact of digital technology on society. This means that in the framework of the Stack, a number of layers have been added which emphasise the common ground that society shares with the Stack, such as the common ground with the user and institutions and that with the material basis of a digital system.

Resources

Although digital systems can reach virtual heights, ultimately, they remain grounded in a material basis. Every system consists of certain resources, such as standard elements as steel, glass, silicon, gold, but also new materials such as graphene. Furthermore, in this layer we also include the use of energy and space. Although this seems far removed from the reality of apps, smartphones and social networks, this physical base partly determines the economic, social and geopolitical dimension of the Stack. For instance, strategic interests and energy costs play an important role in the location selection for server parks.

Hard infrastructure

From the aforementioned resources, all infrastructural hardware elements are built that make up the Stack. Think of hardware for storage (e.g. hard drives, solid state drives, magnetic tape), computing power (CPU, GPU), transmission (5G antennae, fibre optic cables) and measurement (optic sensors, microphones). Thus, this layer forms the rough computational basis for the possibilities in the rest of the Stack.

Soft infrastructure

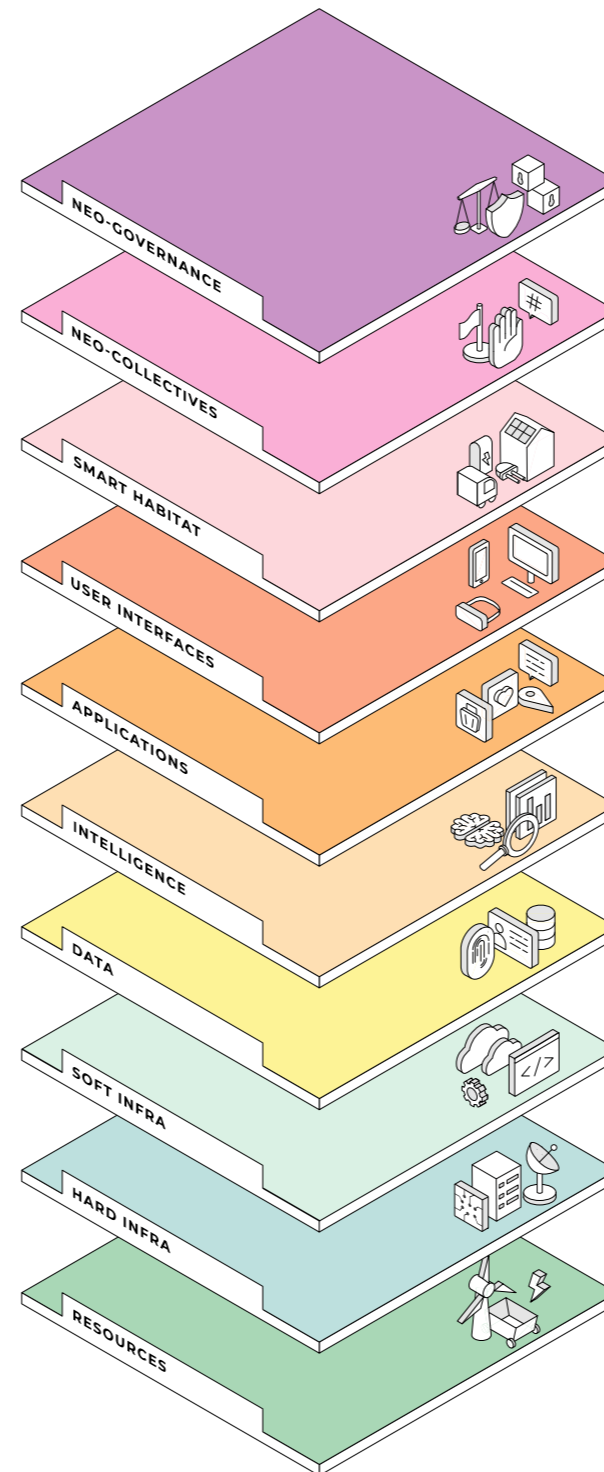
On top of the hard infrastructure, we find the modular software building blocks that relate to the direct control, connection and virtualisation of hardware (e.g. firmware, network protocols, kernels, operating systems and middleware), the development, management and use of databases, the organisation of the business logic or the way information is eventually presented to the user (presentation layer or front-end). Aside from the fact that this layer provides the virtual semi-finished products for software development, the codified administrative rules of software ecosystems that are built on top of it are also determined here.

Data

A digital system is meant to store, send, process and present data. In this layer we define the precise nature of the data. A digital system may work with personal data (behaviour, emotions, features) or more contextual data (weather, location, time) or data from more abstract actors (company data, government data). Furthermore, this layer also looks at the volume, variety, reliability and validity of the gathered data in a system. These features in turn determine the quality of smart algorithms that are trained on these datasets..

Intelligence

In this layer, there are the "smart" algorithms that are capable of automatically developing prediction models based on training data. Think of algorithms that are able to recognise objects (machine vision, image recognition) or speech (NLP, voice recognition). These algorithms can then be used within services to scalably offer smart functions to the end user, such as a voice assistant.



Services

All the aforementioned layers amount to a fully-fledged service for the end user. A service could take the form of a platform that brings together supply and demand (e.g. the sharing economy) or where communication occurs. A large share of the services only relates to the domain of information (such as communication or the streaming of content) but can, naturally, also relate to the physical world (e.g. online shopping or ordering a taxi).

Interface

Users ultimately approach services through various user interfaces. The user interface is the intermediary technology required for the user and computer to interact. This interaction may occur along all kinds of different modalities such as vision (screen, VR headset), speech (voice assistant), gestures (3D cameras) and hearing (wireless earphones). On the one hand, user interfaces are a determinant of the information and experience that digital systems can convey, and on the other hand of the type of data that can be gathered about the end user and their environment.

Smart Habitat

Our increasingly smart living environment forms an interface between society and the digital Stack that facilitates those services, provides us with information and derives data from us and our activities. This makes our living environment a source of data, but because of digitalisation in various sectors and the addition of robotics, our living environment itself is becoming more dynamic and responsive.

Neo-collectives

As digital technology further pervades our lives, the impact of the Stack on social structures is intensifying. Thus, from the Stack, and the digitalisation of daily life, new political and cultural collectives are arising, while these neo-collectives in turn (re)shape the Stack socially. As such, it is analytically useful to consider these collectives an integral part of the Stack.

Neo-governance

Because of new technology, new institutional structures are arising as well, such as digital forms of participation, decision-making, but also enforcement. This allows for the emergence of new models of governance that also pertain to governing the Stack itself.



The Stack from a historical perspective

In order to understand how, in the coming decade, the convergence of developments on different layers may lead to great change, we only need to look at the past. To illustrate, we will discuss a number of important moments of computer history, to get a sense of how convergent dynamics between the layers of the Stack can lead to disruptive phases of progress.

During the Second World War, the first electronic digital programmable computers were developed. Because of the large number of electron tubes and relays (hard infrastructure), these machines were large and heavy. For instance, the ENIAC – the first Turing-complete, programmable computer in the U.S. – weighed 27 tonnes and occupied 167 m². Moreover, these machines had to be operated by means of complex switchboards (user interface) that required a profound knowledge of mathematics and technology on the part of the operator. These computers were thus only used to serve highly-strategic national interest (neo-governance). In the next twenty years, we saw this change with the advent of mainframes and mini-computers, in which the combination of more powerful processors (hard infrastructure) and batch-processing software (soft infrastructure) already made it possible for multiple users to share one computer at the same time through their own terminal and keyboard (user interface), also known as "time-sharing", which made computers more widely deployable for larger businesses and universities (neo-collectives).

This extremely centralised form of computation slowly gave way to decentralisation of computing power in the '80s. Moore's law, the rule the semi-conductor industry had imposed on itself that "prescribes" that the transistor density of an integrated circuit (hard infrastructure) should double every two years, led to a degree of miniaturisation and price decrease that it became lucrative to sell smaller computers to individual households. However, it was not until an operating system (soft infrastructure) was introduced that could be operated with a mouse and graphical user interface (user interface), in combination with a suite of useful applications (services), that the personal computer became attractive to the ordinary home user (neo-collectives).

With the widespread distribution of PCs in the following years, the foundation was laid for another historically convergent moment in computer history – the rise of the World Wide Web. While business mainframes evolved into desktop computers, the U.S. army's research institute (Advanced Research Projects Agency) developed the ARPANET that connected army computers to each other. Against the backdrop of the Cold War, a collection of network protocols was developed known as TCP/IP (soft infrastructure), which, with its open and distributed packet switching network architecture should be able to withstand nuclear attacks.

In the '80s, British computer scientist Tim Berners Lee from CERN added to this an application-oriented protocol (Hypertext Transfer Protocol) and mark-up language (Hypertext Markup Language). This allowed for documents and files to be linked to each other in an open

and standardised way and made it possible to search them (soft infrastructure). Combined with the widespread adoption of PCs (user interface), this enabled sufficient network effects and open innovation to arise for both internet providers (hard infrastructure) and web services (services) to become viable, which in turn fostered the rise of the commercial web. With the advent of broadband internet (hard infrastructure), we also witnessed the appearance of rich multimedia internet services such as video and gaming platforms (services).

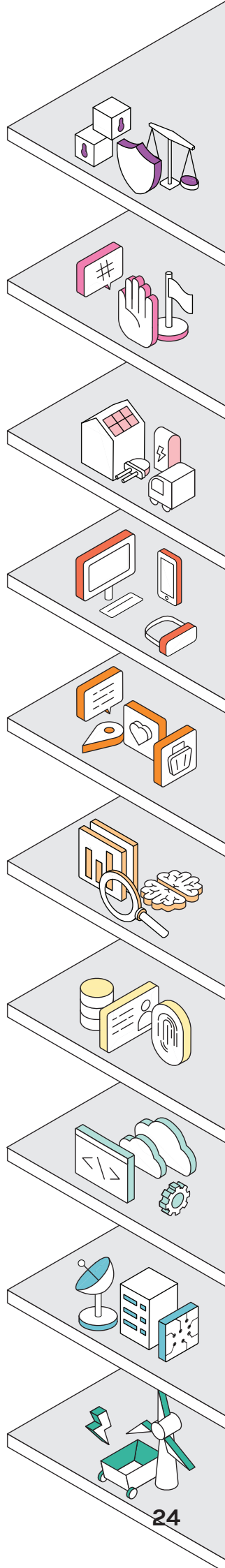
We recently saw a similar dynamic with the rise of the mobile web. Although pocket PCs and Internet Communicators had been on the market since the '90s, it was not until 2007 that we saw the first successful phones with Internet connection in the form of the smartphone. Its success was partly caused by the combination of a user-friendly touchscreen interface (user interface), 3G broadband connection and powerful, energy-efficient processors (hard infrastructure) and an attractive ecosystem of developers of services (soft infrastructure), which then led to an explosion of mobile applications.

Moreover, the development of mobile applications was boosted by the rise of cloud computing in 2006. Whereas cloud providers benefited from the advantage of scale by "virtualising" servers, service developers soon had the advantage of not having to make any large risky investments up front and the cloud infrastructure could easily be scaled up as data traffic increased. It is only with the widespread adoption of the smartphone that we can really speak of the era of the personal computer (neocollectives), as the original personal computer was mainly linked to a household.

This new paradigm also promoted the centralisation of market power, which is now visible in the dominance of a small number of technology companies. In turn, this led to a more critical stance on the part of governments towards these tech parties, in the form of stricter policy (neogovernance).

In the slipstream of the rise of the internet and the web, we also witnessed the revival of artificial intelligence (intelligence). The discipline that was in hibernation, so to speak, since the early '90s due to lack of progress and budget cuts, has experienced enormous acceleration in the past decade. Deep learning, an AI method that, conceptually, has existed since the '70s, has profited immensely from the explosive increase in data, partly by virtue of the internet (data), and because of the growing parallel computing power (hard infrastructure). Thanks to this revival, these algorithms can be found in many of our services, from search engines to voice assistants (services).

This brief tour of computer history shows that every layer has its own dynamics. For a long time, the semi-conductor industry (hard infrastructure), for instance, saw the exponential growth of Moore's law



practically non-stop. Other layers, such as the intelligence layer, have had moments of relative stagnation due to the concurrence of technological, institutional and economic setbacks. Furthermore, we have seen that the most disruptive developments arose because of the convergence of developments in various layers of the Stack. We see that the layers of hard and soft infrastructure and of intelligence make up the foundation for new forms of information sharing and processing, but developments in the user interface layer are especially pivotal regarding the extent to which these functions eventually appeal to the end user. It is exactly these lessons we try to keep in mind when we consider the trends of the coming decade.

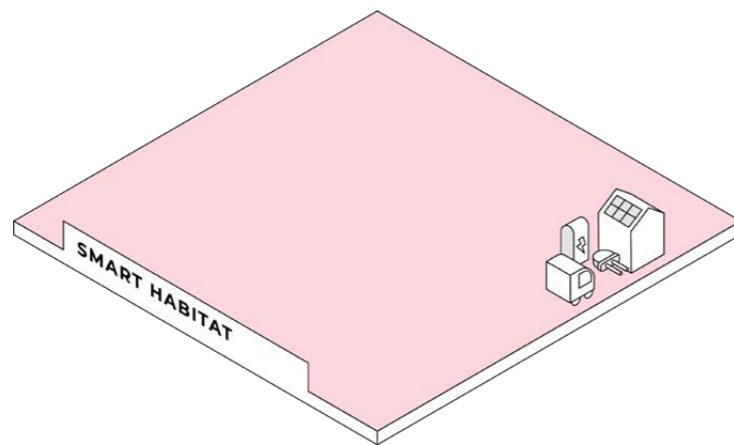


Chapter 3



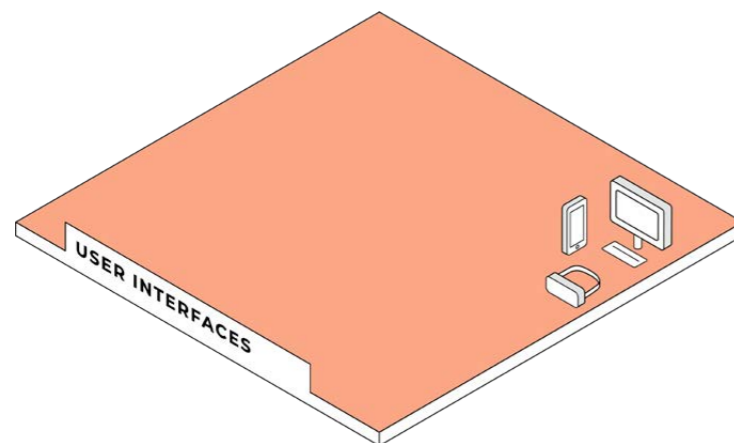
The digital Stack in 2030

On different layers of the Stack, we see technological developments that will partly shape our digital future. These developments, and the accompanying uncertainties, will be elaborately discussed in the "Deep Dive" at the end of this document. Here, we will limit ourselves to the main themes per layer of the Stack. We will only discuss the eight layers that are essentially technological in nature.



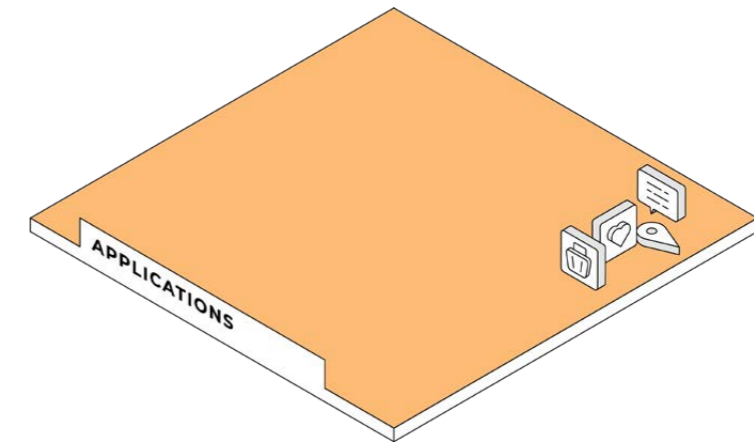
Smart Habitat

The addition of sensors and interfaces makes our living environment an integral part of the Stack. This yields data and insights, but it also means that our living environment is becoming increasingly interactive and personal, as well as more meddlesome and forceful.



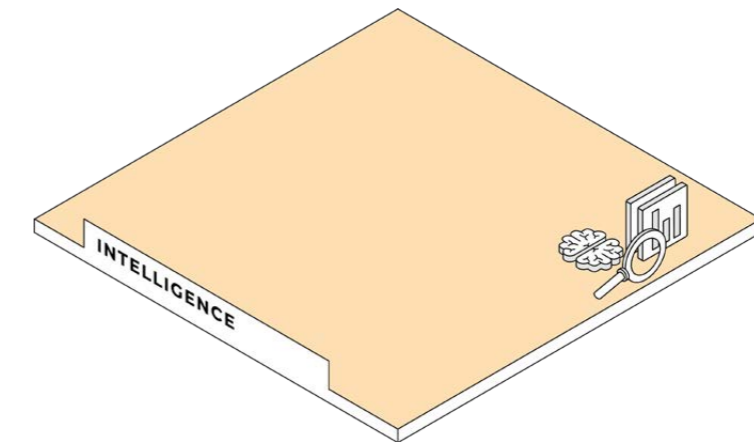
Interface

The interfaces between us and the underlying Stack are becoming more versatile, more intimate and subtler. The computer is disappearing to the background, giving rise to a more intuitive, accessible and richer experience. At the same time, this technology may be perceived as invasive and privacy, autonomy and physical integrity are under pressure.



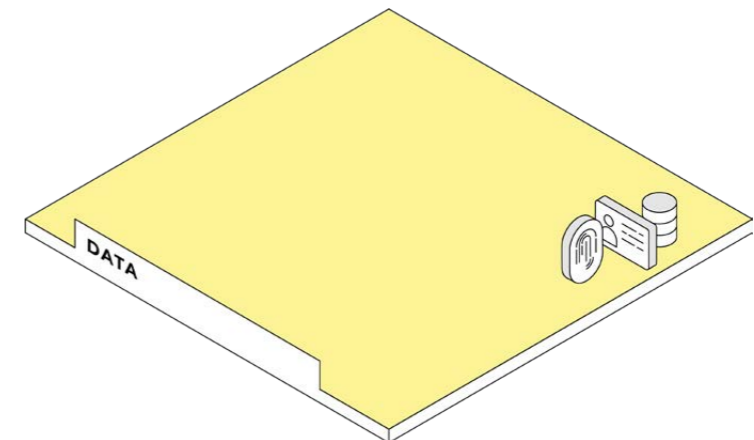
Applications

Due to the integration of various services behind a single interface, digital ecosystems are emerging in which users are offered a personalised, frictionless experience. This, however, raises the question who sets and enforces the rules within these (international) ecosystems and what role governments should play in this.



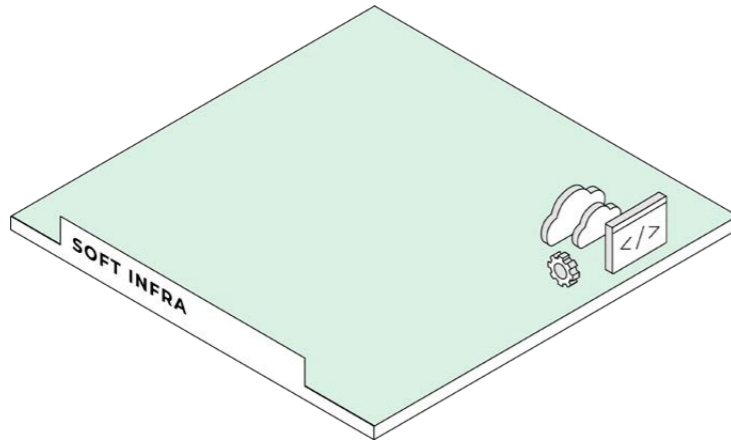
Intelligence

The applications of AI are expanding, and these systems are becoming more creative and will increasingly operate independently. AI systems are becoming more versatile and more easily adjusted to our norms and values.



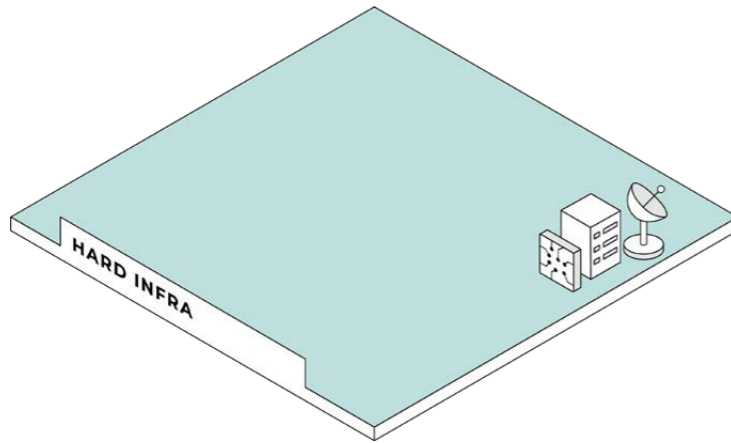
Data

The amount of data available is increasing because of our use of digital services and the addition of sensors to our living environment. This data offers real-time insight into behaviour, objects and processes and creates possibilities for direction. At the same time, it raises the question which problems this data should and can solve.



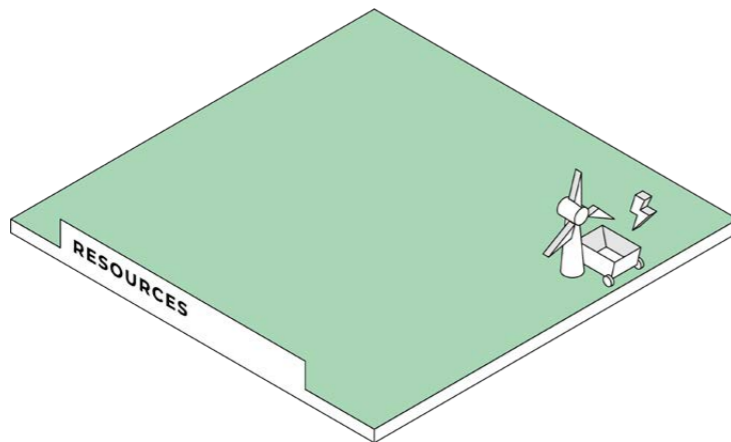
Soft infrastructure

The concentration of power with a limited number of platforms cannot be separated from the protocols that underlie the Internet. Various alternative protocols are attempting to correct this structural flaw and, for instance, give citizens more control over their data and safeguard equal opportunity for new providers.



Hard infrastructure

The costs of hardware continue to drop exponentially, and new technologies are offering the computing power and connectivity required for applications of artificial intelligence and the next generation of digital services. The advent of quantum computers will lead to breakthroughs in specific tasks such as modelling and searching large amounts of data.



Resources

Recycling resources and using less scarce or environmentally harmful materials could make the Stack more sustainable and just and decrease the dependency of foreign suppliers. The Stack's energy supply will have to become more sustainable as well.

Chapter

4

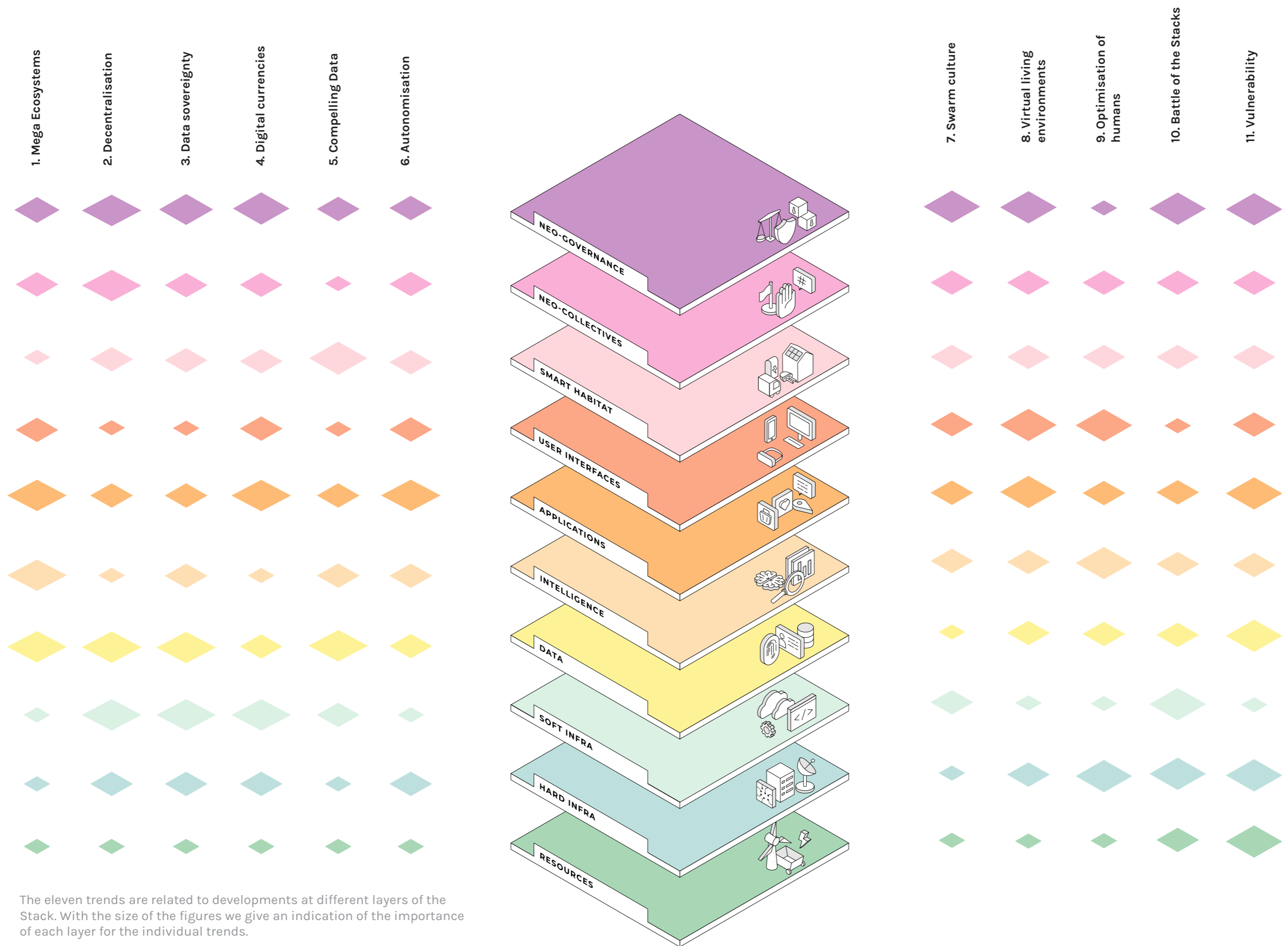


4

Trends and development paths

These trends arise from both technological developments as well as societal movements. In part, they are the result of technological possibilities that fulfil a (latent) societal need. In a number of cases, this pertains to developments that are already underway but will accelerate or converge with other trends in the coming years. At the same time, we also identify a number of trends that are in fact a response to the current state of affairs in digitalisation, as exemplified by attempts to break down the market power of the large tech companies.

Each trend will be introduced based on technological developments and the societal, economic and political drivers behind them. As each trend knows several uncertainties in itself, we translate each trend into two divergent development paths. These paths show how the trend will develop in the future and which factors may be decisive in this. In a number of cases, these development paths relate to the question whether a trend will actually persist and lead to a paradigm shift or only to incremental change. With other trends, the question is rather what particular shape a development will take, and, for instance, which actors will be in control.



The eleven trends are related to developments at different layers of the Stack. With the size of the figures we give an indication of the importance of each layer for the individual trends.



Trend 1: Mega Ecosystems

Digital platforms bring together various services in a single interface and raise the added value by using data sharing and intelligence to align these services with each other. Eventually, this will result in a limited number of ecosystems within which consumers will be able to organise and integrate a considerable number of their daily practices.

All big technology companies are working on the integration of various services into a single interface. They want to give their users an optimal user experience and keep them within the bounds of their own ecosystem as much as possible. A good example is the Chinese WeChat, which has developed from a chat app to a super-app and gives users access to all kinds of services. WhatsApp (Facebook) could develop in the same direction. Google (with Google Maps) and Amazon too are continually expanding their services, both the digital as well as the physical (e.g. with books on travel or physical stores). Further development of digital assistants will contribute to this trend as they directly refer consumers within the ecosystem.

The integration of different services and the exchange of data in an ecosystem enables tech companies to offer personalised services and align them with each other. The appeal of this kind of service range quickly leads to strong scale and network effects and thus a "winner-takes-all" dynamic: more users within an ecosystem means more data, which can be used to provide even better services. For individual service providers, from taxi drivers to insurers, it will become easy to "plug in" their products into an ecosystem, gain access to the required data and cooperate with complementary service providers. The drawback to this is that they will lose direct contact with their users and could become anonymous, replaceable "white-label" suppliers. This could have huge consequences for local employment opportunities and result in working conditions being increasingly dictated by international platforms and their competition for the user's favour.

As data exchange is a condition for the integration of services in the ecosystem, questions have arisen relating to data ownership, privacy and autonomy. In addition, the power of ecosystems could increase to an undesirable extent, if they, for example, exclude certain services (or users). A centrally orchestrated ecosystem, in line with the business models of today's tech giants, therefore seems undesirable.

Development paths

Large American and Chinese tech companies are particularly well-positioned to give shape to ecosystems. They have the market power and the technological ability to attract and hold on to the business of different service providers (exclusively), have them mutually exchange data and use artificial intelligence to offer users optimal, frictionless services. Besides concerns over the use of data and loss of freedom of choice for users, there is the risk that a large share of Dutch companies will be subordinated to the interests of tech giants and eventually become anonymous ("white-label") suppliers that have to offer up tens of percent of their profit to the ecosystem in which they operate.

The increasing power of large tech companies stimulates smaller (Dutch and European) companies and governments to work together and start their own, more open, platforms. In order to offer comparable functionalities and achieve integration of services within an ecosystem, broad alliances will have to be forged with companies from different sectors. The infrastructure that underlies these ecosystems could have the character of a utility function and be (semi)publicly managed.



Trend 2: Decentralisation

The growing resistance to the power of large tech companies has opened the door to radical alternatives to the current centralised internet. Based on new design principles, according to which institutional innovation is embedded in technology, decentral solutions are emerging for matters such as data storage, intelligence and various kinds of transactions in which there is no room for powerful intermediaries.

In the '90s, the Internet was seen as a liberating, levelling and democratising force. The key protocols of the Internet, after all, enabled everyone to build "anything" on top of this global decentral network. This form of open innovation has led to an explosion of services and products. However, as a result of strong network effects and limited supervision, a small number of players has a dominant role in setting the rules of play. Moreover, they disproportionately profit from the digital economy. All of this has negative effects on society: obstruction of open innovation, violation of privacy, mass manipulation of users and a disproportionate concentration of power are only a few of the evils caused by this development.

In response to this, the open-source community is working hard to devise new Internet protocols. They fall under the heading of "decentralised web", or web 3.0 and are expected to pave the way for a new generation of open and fair services. Technologies such as blockchain, consensus protocols, utility tokens, smart contracts and PET (Privacy Enhancing Technologies) ensure that central and powerful platforms are no longer entrusted with a number of critical functions. Instead, they contain a decentral protocol layer that, like a utility, is available to everyone who wants to use it. This mainly concerns functions such as data storage, data sharing, data processing, data validation, identity and transaction traffic. The idea behind this development is that technology giants lose their oligarchic position and the parties concerned can make decisions together about the future of the Internet and digital services.

The essence of the new protocols is that principles such as data ownership, data sovereignty and privacy are already ingrained in the design of the technology and upholding them does not require agreements or regulation.

Eventually, so-called Apps, or decentralised consumer applications, may even come into existence. Examples of this could be a decentralised replacement of Facebook, whereby, in accordance with the stakeholder model, the social network would be governed by both the developers and the users. Even users could then have a say in the way a platform is organised.

Development paths

Web 3.0, with its decentral architecture, becomes the new standard. All kinds of services, from social media to financial services, are able to use data insofar as they obtain consent from their users, but do not own that data and are not be able to sell it to third parties. Moreover, the users are co-owners of the service and have a say in and profit from future developments. This leads to the big tech companies (partly) being sidelined: protocols take over the "trust function" from existing online platforms, which lose their powerful position as trusted intermediary. The same applies to traditional players in the financial field, logistics and media, which play a comparable intermediary role. Eventually, the decentral and consensus-driven organisation model may have far-reaching effects on society and lead to other forms of participation and governance, in which elements of direct democracy and real-time decision-making play a larger role.

The web 3.0 clashes with existing ideas, interests and structures. Not only those of tech companies that are losing control over their data and users, but also of governments that are at risk of partly losing their hold on the digital sphere. Moreover, it is uncertain whether users will embrace this technology and these forms of shared responsibility. It is therefore conceivable that these solutions will remain limited to relatively small niches in the market or that only a few elements of the technology will be adopted, while any radical change remains absent.



Trend 3: Data sovereignty

The increasing importance of data in achieving economic and societal goals results in a different way of thinking about the value and accessibility of data. Citizens, companies and governments gain data sovereignty and are thus enabled to make conscious decisions about the data they make available to others.

The importance of data will only increase in the coming years. In part thanks to AI, more insights will be drawn from data, predictive models will be developed, and services and processes can be optimised.

Currently there are, however, two problems pertaining to data: the original data owners have lost ownership and a lot of data is held in sealed silos. Because of this, data is not fully utilised, e.g. for innovation, and public values such as privacy and autonomy are coming under threat. The problem with data ownership is the result of digital practices in which a platform takes possession (either lawfully or not) of all the data and uses it for its own purposes. Consumers and suppliers that have provided or produced the data then lose control over it and do not optimally profit from it. The "silo" problem is the consequence of commercial (or other) interests of the platforms, but also of the lack of an open and standardised infrastructure for sharing and/or trading data.

Solutions to both problems are in the making. First, new architectures for managing data, such as data vaults, could enable consumers and (supplying) companies to exercise more control over the use of their data. That is, they would gain data sovereignty and be more fairly compensated for the data they offer or provide one-time access to.ⁱ That could mean that users put up their data in exchange for (demonstrably) better service, or a financial incentive, but also that they can share data for the benefit of society (so-called data altruism).

Second, standardised protocols for data sharing offer an open alternative to the sealed silos of current platforms. This could facilitate equal access to data for different players. Naturally on the condition that the original owners have given their consent. Various European initiatives are ahead of this, such as Gaia-X when it comes to standardisation in the cloud, different shared "data spaces" (e.g. for healthcare and transportation) and the Data Governance Act.

Development paths

New architectures for the management of data take the market by storm as a result of growing consciousness among consumers and service providers, who understand that the current model of data silos is not tenable for them either. The latter applies to virtually everyone who wants to start a business outside of the large ecosystems. For them, the mutual provision of data, with the consent of consumers, is the only way to survive in a data-driven economy. This model requires consumers' awareness of the advantages and disadvantages of sharing their data, with companies, but also with governments. New service providers play into this by developing their own digital data coaches. Governments have to find a new balance between their own need for data and protecting consumers from data-hungry parties.

Though the current policy of privacy protection and sharing public data limits the power of large platforms, it does not yet lead to the breaking open of silos. Consumers, however, continue to opt for "free" services and the convenience these parties offer and are not willing to make the "sustainable" choice for paid services or services that are otherwise limited by their conscientious handling of data. The lack of infrastructure for sharing data on equal footing maintains the status quo and keeps data access limited for smaller start-ups, scale-ups and public initiatives.



Trend 4: Digital currencies

Cryptocurrencies could potentially enable transactions without the mediation of banks at very low cost. This gives rise to new revenue models and remuneration structures. At the same time, digital currencies can disrupt financial markets and sideline existing players and watchdogs.

The current focus on Bitcoin as a speculative investment, as well as the discussion on its exorbitant use of energy, are distracting us from the underlying forces and the technological possibilities of digital currencies. Balance sheets in cryptocurrencies are kept track of in a so-called distributed ledger, generally an open blockchain infrastructure. Essentially, all participants in the network have equal rights and an equal say in the governance of the currency. This means that banks and governments have far less control and that users can trade these coins away from supervision.

The growing popularity of cryptocurrencies could come to undermine the role of commercial banks, as well as that of central banks. The more often digital coins are earned and spent online, instead of being bought and sold with euros or dollars, the farther they get out of sight of tax authorities, and the more challenging it becomes to collect taxes.

At the moment, concerns about cryptocurrencies mainly relate to illegal transactions and money laundering. In time, however, these currencies could also pose a threat to the stability of the financial system. In case of currency fluctuation, a user-friendly cryptocurrency with billions of users worldwide, as Facebook envisioned with the Libra project, could lead to real problems for the fiat currencies (and bonds) linked to it.ⁱⁱ It is therefore not surprising that several commercial and central banks (such as the ECB, but also China and Brazil) are already working on their own digital currencies, in an effort to maintain control of the financial system and to fully exploit the benefits of cryptocurrencies, such as the low transaction costs and traceability of transactions.

Cryptocurrencies could also lead to major changes in a practical sense. In theory, crypto coins make it possible to make payments at extremely low cost and with rapid settlement. This would make it profitable to charge very small amounts for services or products, such as reading a social media message or supplying self-generated energy. Moreover, it would be possible to register ownership of all kinds of material and non-material matters (such as data) on a blockchain and make it easily tradeable (so-called tokenization).

Cryptocurrencies can also be designed in such a way that, similar to a voucher, they can only be used for specific purposes.ⁱⁱⁱ For example, they could only be spent in certain web shops or on specific products (such as products with a sustainability or fair-trade label).

Development paths

Cryptocurrencies on a public blockchain cause a revolution in the financial system as they enable businesses and consumers to transact with each other without the intervention or control of third parties. In doing so, they rely entirely on the technology used and the power of distributed decision-making. It is precisely because these public blockchains benefit from strong network effects and open innovation that they gain strength. Companies and other organisations that do not participate in this and do not connect their systems to the public infrastructure, lose relevance.

Although the potential advantages of crypto coins (low transaction costs, the use of smart contracts and distributed storage of data) are embraced, management and supervision remain in the hands of a limited number of parties such as governments, but also companies that want to use a currency within their own ecosystem to reward customers or suppliers. These so-called private blockchains, then, are the result of the desire to keep control of the financial system. Moreover, some (institutional and private) users place more trust in traditional parties and regulators than in public cryptocurrencies.



Trend 5: Compelling Data

Smart houses, cities and factories are generating a flow of data. With the help of artificial intelligence, this data will make our living environment increasingly predictable and more easily governed. This development raises the question which problems we can and want to solve with it, which data is required for this and how we can limit the "power" of data.

The promise of the data-driven society is that data forms the basis for smart systems that are more efficient, more effective, cheaper and cleaner than the current "dumb" systems. With the increase in the number of sensors and connected devices, the amount of data will also increase, from which we can derive new insights and which can provide us direction. The assumption behind the data-driven society is that it will lead to a more rational society in which reality becomes transparent and solutions to all kinds of problems will logically present themselves. In practice, however, we will face several challenges.

First, the increase in the amount of data does not necessarily mean that all data is equally relevant. For example, there is a good chance that all kinds of sensors will become so cheap that they will be included in products by default and, with the advent of 5G and other network technologies for the Internet of Things, will become interconnected. The data from these sensors would then become available to us without it being necessarily clear in advance what purpose it should serve. The same applies to data from digital services; endless data will become available, but the distinction between meaningful and meaningless data is difficult to make.

Second, data and the insights derived from it will come to partly determine our thinking and our actions. AI is expected to help us discover patterns in raw data and glean useful insights from them. However, this could also lead to unexpected and sometimes unwanted or uncomfortable insights. The dangers of data manipulation ("fake data") also lurk. Once certain insights based on data and AI have been gained, we cannot simply ignore them and will have to act on them. This applies, for example, to data on (the consequences of) environmental pollution or road safety and could lead to politically sensitive issues. Third, more insight does not necessarily lead to simple or neutral solutions.

Data can help to (better) chart and understand problems, but that does not guarantee an immediate solution. For example, data could help establish that the waste containers in a particular neighbourhood are always full, but in order to solve the problem, the municipality would have to invest in its waste collection service. No matter how much data is available, actually solving problems nearly always requires making (political) choices: which problems are urgent and what price are we prepared to pay for them to be solved? Insight into mobility behaviour could create possibilities for solving congestion problems, but this would likely require political choices regarding, for example, road pricing.

Development paths

The large-scale application of sensors and data collection, in combination with intelligence, makes it possible to develop "digital twins" of cities, factories and subsystems for, for instance, energy and mobility. Widespread faith in technological solutions to all kinds of societal problems reduces these problems to what is measurable and controllable. This technocratic approach leads to incremental solutions, such as improved energy-efficiency and smarter allocation of goods and people. This approach, however, does not suffice when it comes to structurally tackling problems such as inequality of opportunity and climate change. For that, strong political choices remain necessary, as is the case with road-pricing, for example, and citizens and companies must be willing to change their behaviour.

Data analysis and the insights gleaned from smart cities and production processes make it abundantly clear that existing practices are untenable and that structural change is necessary to shape a just and sustainable society. In this way, data contributes to the political support that is needed for this more radical form of change. Incremental technological improvements remain necessary but are only the beginning of a much deeper transition in which behavioural change and new social and economic "rules of play" are leading.



Trend 6: Autonomisation

While AI has so far mainly been used to analyse, predict and make suggestions, AI systems will come to act more independently in the coming years. Initially, this will be limited to "harmless" applications, but gradually, AI systems will come to perform more complex tasks and more deeply pervade our lives.

The rise of artificial intelligence in both software and hardware applications poses major ethical questions to society. To date, the focus has mainly been on the extent to which and the ways in which these systems may be biased and disadvantage specific population groups. Think of systems that, consciously or unconsciously, have been trained with "biased" data, predominantly including the faces of white men, for example. The controversies surrounding this kind of systems sometimes lead to bans, such as the ban on the use of facial recognition technology by police forces in a number of American cities. However, the development of technology continues at an unabated pace and will lead to new manifestations of AI entering society.

Increasingly, this will concern systems that are not intended to make us function better per se, but to take tasks off our hands immediately. The most obvious example is of course the self-driving car, but there are many more "dull, dirty and dangerous" tasks that we would like to outsource to machines, because there is a labour shortage, for example, because we want to increase our safety or simply out of a need for luxury.

As attractive as this idea is, there is another side to the coin. Although the term "autonomy" suggests that we're dealing with independently (and sensibly) operating machines, these systems will usually be deployed for a commercial (or political) purpose. This is not necessarily a problem but could have undesirable consequences, such as discrimination, violation of privacy (through surveillance), or concentration of power. In abstract terms, the use of autonomous systems will always limit human autonomy, either because we relinquish control, or because the system tells us how to drive.

The message of Europe is therefore that human values must at all times be central to the development and deployment of AI ("human-centric AI") and that people must "maintain meaningful control" over the actions of a (semi-)autonomous system. However, the question is whether this guideline will remain tenable in the long term and whether we will not be tempted to give these systems more autonomy, because they, for example, simply perform (measurably) better than people do.

Development paths

The obvious added value of autonomous systems for companies, governments and consumers leads to a widespread embrace of the technology. Initial concerns about security, algorithmic "bias" and loss of human autonomy fade into the background and standards of use of the technology shift. Regulation and enforcement therefore focus on limiting immediately visible problems but cannot prevent the development of AI from having adverse consequences in the long term, such as the (inevitable) loss of human autonomy.

Society develops a very critical attitude towards autonomous systems. This attitude is motivated by mistrust of the large technology companies and governments that develop and deploy (monetize) AI systems. As a result, acceptance of the technology takes more time and remains limited to applications that clearly add value and whose side effects are easily estimated. This slower pace gives society the opportunity not only to build trust in the technology, but also to make demands as to the design of systems.



Trend 7: Swarm culture

Digital platforms bring people together, introduce new forms of collaboration and thus contribute to the emergence and spread of new ideas. This dynamic will accelerate in the coming years, among other factors because of the advent of new interfaces and low-threshold applications of artificial intelligence.

Social networks create value by mobilising people, making it possible to share goods or providing a breeding ground for ideas. This value can take the form of (harmless) entertainment, such as TikTok dances or "challenges", but can also be socially or politically charged, such as the Black Lives Matter and #MeToo movement, the QAnon conspiracy theory or the r/wallstreetbets investing community on Reddit, which recently caused the volatility of various stocks. The power of these types of movements will grow, but at the same time they will also become increasingly elusive, in particular due to the advent of freely available AI, with which almost anyone can manipulate and then distribute image and sound as they please.

Societies are faced with the challenge of combating the excesses of this online dynamic without losing the positive aspects in the process. Undesirable developments will be curtailed in various (legal) ways, possibly Europe-wide, while desirable behaviour will be stimulated (financially). Microtransactions can be used, for example, to reward the sharing of knowledge or goods. Social networks will also be used to train benign AI systems, to facilitate "open source" development of hardware and software and to bolster cooperative platforms. Financial incentives contribute to this in the form of directly rewarded behaviour or distributing the proceeds of collective efforts proportionately among the participants.

The arrival of new interfaces will also make it easier to influence behaviour in the physical world. For example, it is conceivable that augmented reality glasses will be used to encourage wearers to choose a quiet route through the city or to help them in the event of a calamity. The hybrid physical-digital game Pokémon Go can be considered a forerunner of digital network dynamics drawing in users in the physical world to such an extent that they get carried away.

Development paths

The advantages of the online society outweigh the costs and through limited control and management, platforms succeed in eliminating the greatest excesses of disinformation, incitement and cons. As a result, the internet largely remains a haven of unprecedented opportunity for knowledge sharing, creativity and entrepreneurship. Increasingly, AI developers use the power of the online masses to train their systems and tailor them to the needs of users.

Society concludes that the internet should be seen in part as a failed experiment and that online platforms should be heavily curtailed. The scale and network effects of digital technology allow adverse effects to spread quickly and widely. The normal rules that apply to the physical world, with regard to freedom of speech, for example, do not suffice here. That is why stricter rules are applied online, such as limiting anonymous participation and the possibility to endlessly share content.



Trend 8: Virtual living environments

The worlds of social media and games will become a place where people can have meaningful experiences. This partly concerns practices we will move from the physical to the virtual world, such as playing, learning and working, but new practices will emerge as well.

Futurists and science fiction writers have been fantasising for decades about virtual worlds where people are completely absorbed in a digital reality. In these worlds, with or without the help of VR glasses, they experience endless possibilities to develop activities and to devise an entirely new identity for themselves. As of yet, initiatives that try to make this fantasy a reality have had little success.

There are now a number of games that have managed to create a virtual world where players can do much more than just play the game. Games such as Fortnite, Minecraft and Roblox have evolved into environments that their (mostly young) users experience as complementary to the physical world: they can "hang out" there without playing the game and gain meaningful experiences. This is perhaps illustrated most clearly by the virtual live performances given by various artists in Fortnite, which attracted millions of visitors and really made the spectators feel as if they were present at a live concert. New generations of VR goggles, clothing (e.g. gloves) that provide haptic feedback, and AI that allows environments and characters to be created real-time will contribute to an ever-richer experience.

As these worlds become more significant in the daily life of a growing group of users and as more everyday practices are "moved" there (e.g. going out or education), the demand for regulation and enforcement will naturally arise. What is allowed and what is not allowed and who decides this? These environments will most likely be international, and the question is what role Dutch law will play here, and in a broader sense, Dutch norms and values. Essentially, these are the same questions that are already relevant with online platforms, but that become more pressing when it comes to virtual worlds.

However, as this technology evolves, the risk increases that people will lose sight of the relationship between the physical and the virtual world. This could have major implications in terms of game addiction, cyberbullying and the spread of disinformation.

Development paths

The latest generation of games offers players and developers more freedom. Users come to shape their online living environment more and more and thus become producers as well as consumers. Education and work increasingly take place in this world, or these worlds, as do nightlife and festivals. The old fantasy of unlimited possibilities in a so-called metaverse, as we know it from science fiction, finally takes shape. Because these worlds have no physical boundaries, it is mainly the companies behind the platforms that determine and enforce the rules. This means that they increasingly enter the jurisdiction of traditional governments.

Virtual worlds develop along the lines of the physical world. Instead of anonymous, global platforms where everyone meets everyone, virtual spaces emerge that - like a collection of WhatsApp groups - support and enrich existing communities and practices. Large providers benefit from scale and network effects, but there is also room for small-scale and local "franchises" of internationally operating platforms, which are tailored to the local character of communities and meet the need for online governance based on local norms.



Trend 9: Optimisation of humans

So-called intimate technology helps us overcome our limitations. New interfaces offer the possibility to strengthen and augment our senses. We perceive our ever more intimate collaboration with digital assistants to be an expansion of our cognitive capacities.

People have always used technology to overcome their physical and cognitive limitations. In the coming years, advanced "enhancement technologies" will become available with which we will collaborate intimately. These technologies range from robotics for physical support to sensors that provide us with extra senses or digital assistants that act as an extension of our brains.

New interfaces play an important role in this, because they make the interaction with the technology more intuitive and "natural". It will sometimes be the technology directly helping us (e.g. augmented reality glasses that provide the wearer with extra information), but the technology can also be a tool to make ourselves healthier, fitter or smarter. Existing health trackers and the broader "quantified self" movement are elements of this trend.

In addition, the processing of large amounts of data and the application of AI and quantum computing are expected to lead to breakthroughs in healthcare. As a result, we will better understand medical disorders and their causes and will be able to develop and test new medicines and treatment methods more rapidly. Due to the "human enhancement" culture, deeply rooted in Silicon Valley, these resources will not merely be developed to overcome disease or disability, but also to "improve" perfectly healthy people.

It will especially be wealthy citizens and those who have the skills to optimally put it to use who will reap the benefits of this technology. Consequently, the digital divide will deepen further, because access to these resources not only determines what someone can do online, but also has an increasing impact on a person's functioning and well-being in the physical world. The latter implies that freedom of choice may come under pressure. For example, someone who does not want to use the technology, possibly for privacy or security reasons, places herself at a socio-economic disadvantage by making that choice. In a broader sense, moreover, societal norms of health, fitness or intelligence could shift in tandem with the technology, creating a situation in which "non-participation" is even seen as morally unacceptable.

Apart from the issue of equality of opportunity, intimate technology also means invasive technology that could potentially collect and utilise very sensitive personal data, which also entails ethical questions about physical integrity. It might be necessary for governments to protect citizens from themselves and their penchant for self-optimisation, in light of the considerable privacy and security risks involved.

Development paths

The use of "wearables" (such as watches and glasses) and "insideables" (such as sensors) is linked to a growing need to live healthier and more active lives. At the same time, the new interfaces help us to connect ourselves to all kinds of digital services that are increasingly well tailored to person and context. This development threatens to deepen the digital divide between those who can afford the technology and underlying services and know how to fully exploit them to enhance their well-being and development, and those who cannot afford them and lack the necessary skills.

The ever more natural and intuitive use of technology, by means of speech, for example, enables millions of citizens to participate in the digital society and advance themselves. Policy and revenue models focus explicitly on digital inclusion and overcoming physical and cognitive limitations. The Silicon Valley ideal of human enhancement, promoted by American tech companies and aimed at the happy few, does not take hold. This is mainly due to concerns about privacy and loss of autonomy. The solutions for overcoming limitations, on the other hand, are often locally developed and designed to respect those values.



Trend 10: Battle of the Stacks

Superpowers are developing their own Stacks and attempting to elevate them to global standard. This is not merely a battle for economic and international power, but also a battle of ideas about the way we organise our society and the role we assign technology in this.

The freely accessible world wide web does not exist. Different superpowers have their own Stack in which political and cultural ideas are expressed. For example, China has a highly centralised Stack in which the state is the dominant actor, while in the U.S., the free market rules the web just as it rules the economy. These ideas are visible in specific protocols and services, but also in the use of autonomous systems, the handling of data, and ideas about privacy.

With its Golden Shield and the Great Firewall, the Chinese government has been working on its own cyber sovereignty since the late 1990s. In addition, from the introduction of new core protocols and infrastructure (5G) to the development of internationally popular services (e.g. Alipay, WeChat, TikTok), technological global players with which Chinese "soft power" can be exercised, the country is building strong digital dominance on various layers of the Stack.

In the United States, the federal government is struggling with the free role of the big tech companies, the market power they have built up and the way they (could) abuse it at the expense of their users. At the same time, these companies are crucial to the U.S. economy and contribute to the nation's international economic and cultural dominance.

Europe does not have its own Stack yet, if only because the American tech giants dominate every layer of the Stack here. In recent years, however, Europe has begun to shape its own Stack and to introduce the necessary measures to this end. Of course, the GDPR is an important step in this direction and the proposed Data Governance Act and Digital Services Act furthers the pursuit as well. In this way, Europe is attempting to ensure that the European Internet complies with European norms and values, while also contributing to the achievement of broader policy goals related to comprehensive well-being. With these initiatives, Europe may be a role model to other parts of the world and European companies could benefit if European standards are implemented worldwide.

In the coming years, these Stacks will probably grow further apart, and the various power blocs will try to raise their own standards to world standard so as to gain economic and political power. The question is therefore to what extent European ideas will meet with acceptance and can be determinative.

Development paths

The Chinese and the American Stack grow further apart and the exchange of data and mutual use of services decreases to a minimum. In the absence of its own alternative, Europe remains largely dependent on the American Stack. Meanwhile, Chinese influence in standardisation organisations grows, leading to a break between the Chinese and the American-European bloc and further loss of interoperability. However, much of Europe still has an interest in open lines with China and therefore also sees the necessity of adhering to Chinese standards. As a result of these tensions, the European internet begins to crack and an internal "splinternet" threatens to emerge.

Europe's leading role in regulating the Internet leads to the creation of its own Stack, with European players as well as American and Chinese players complying with European values and rules. Europe also succeeds in translating its ideas about the "Good Internet" into internationally accepted standards. This does not directly result in China and America radically revising their own Stacks and online governance, but both countries are no longer able to impose their technology, and the underlying ideas and interests, onto the rest of the world.



Trend 11: Vulnerability

The digital transition is making us increasingly dependent on technological systems and their developers. As a result, society and the economy are vulnerable in trade conflicts, but also to cyber espionage, sabotage and terrorism. A seemingly insignificant event such as a hack or programming error could have dire consequences.

Our dependence on digital technology has a number of risks. First, we rely heavily on a small number of dominant technology companies. Thanks to a "winner-takes-all" dynamic, these companies tend to be autocrats in their domain, e.g. Google dominating the search market and Facebook that of social networks. In addition, these parties control the cloud environment from which other, smaller parties offer their services. Without exception, the tech giants are foreign, non-European players. This suggests that their interests do not always coincide with ours, that control and influence are limited and that we would be hit hard should these parties no longer be able or willing to serve us.

Second, we are highly dependent on (key) technologies that we do not develop and produce ourselves, such as processors and network technology. This limits our autonomy in the digital transition. It also makes us vulnerable to cyber espionage because we have limited knowledge of the precise technology and any "back doors" that allow developers and security services to view our data and communication.

As society and the economy become more digitised and networked, with the advent of countless Internet of Things devices, for instance, our vulnerability to malicious parties increases sharply and their "attack surface" grows. Both state and non-state actors are out to invade systems in order to sabotage them or steal (or hold hostage) data. The risk of industrial espionage in particular will increase considerably and put the earning capacity of our economy to the test in the coming years. The question is whether we will have enough of a "sense of urgency" and ability to arm ourselves against this, to be a match for the increasingly sophisticated possibilities that our opponents are developing.

The rise of quantum computing plays a prominent role in this. The forms of encryption in use today are liable to be cracked by quantum computers in the coming years and thus no longer provide adequate protection. "Quantum-proof" encryption is available, but still needs to be implemented on time. Even if that happens, large amounts of encrypted data will be able to be decrypted retroactively. Under the guise of "harvest now, decrypt later", various parties, including security services, have intercepted large amounts of data. When this data becomes readable thanks to quantum computers, and state secrets, for example, become public, the consequences of this could be even more dire than those of WikiLeaks or other recent data leaks.

Development paths

Partial decoupling of the European Stack from other global Stacks may be the only answer to the increasing dependence and vulnerability of digital systems. If securing knowledge and systems proves impossible within the existing structures, simply because we are dealing with unreliable partners, then a break is inevitable. This, at least in the short term, comes at the expense of earning capacity and growth, but in the long term it may be the only way to safeguard our comprehensive wellbeing.

The digital future holds continual armed peace. Vulnerabilities cannot be fully covered, but this applies to all parties and a precarious balance arises of mutually assured destruction. This makes it possible to continue the digitalisation of the economy and society, but it does lead to a more critical approach to what we do and do not want to digitalise and the appropriate degree of protection.

Chapter

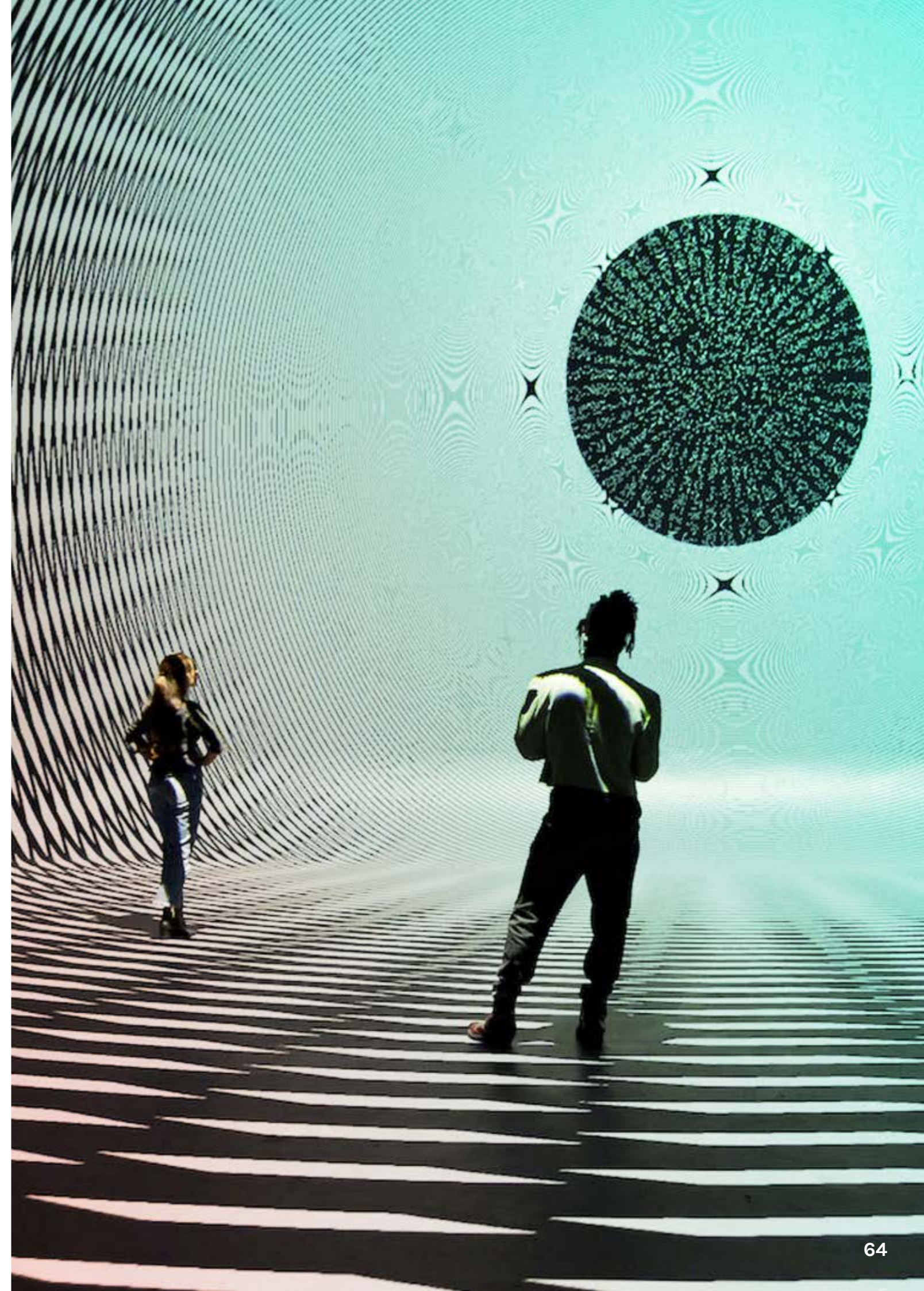
5



Impact of digitalisation

In this chapter, we reflect on the impact the identified trends could have on various policy themes. Per theme, we pose the question how the different trends could have an impact and which variables play a role in this.

First, we take a look at the impact of digitalisation on the earning capacity of the Dutch, and European, economy. It is clear that digitalisation offers great opportunities for knowledge economies like ours, but it may also reduce our earning capacity if big and powerful online platforms sideline (parts of) local businesses and, consequently, profit flows abroad. Second, digitalisation is likely to affect public administration; with regard to implementing and enforcing existing policies, but also regarding new forms of public participation and policy-making. Third, the digital transition could play a role in increasing our comprehensive wellbeing, by creating equal opportunities for citizens and contributing in the fight against climate change and other environmental problems. Fourth, digitalisation raises questions with regard to public and national safety. These questions relate to our increasing dependence on technological systems and the ways in which digital technology can be used against us. Fifth, and finally, the process of digitalisation affects public values. The identified trends offer hope that technological solutions might actually help restore several public values, such as equal opportunity and social cohesion. Yet, at the same time, we should be cautious as to whose values will eventually determine the future of the online society.



Theme 1: Earning capacity

The trends show that changes can be expected in the earning capacity of the Dutch economy. With the Stack model, we can divide the earning opportunities into different dimensions of digitalisation. In doing so, we can distinguish between earning opportunities related to the technology itself and the opportunities that arise if the technology is widely deployed.

If we look along the layers of the Stack, the first thing we see is new opportunities arising in the lower layers, with the realisation of new generations of hard and soft infrastructure. Consider, for example, the development of quantum chips and specialised AI chips, for which new value chains must be set up: this creates opportunities for new players. In the layers geared towards the end user (interface and services), we foresee a steady continuation of the platform economy, which will result in the creation of ecosystems.

The focus will shift from individual platforms to a limited number of integrated ecosystems. The ecosystem with the most attractive range of services and the best user experience will attract the most users and therefore fully benefit from scale and network effects. Existing individual platforms, which currently only offer, say, a mobility service, will therefore have to start thinking about their range of services in order to provide users with a frictionless overall experience. Suppliers of individual services and products (mainly the subcontractors of the platforms, such as taxi drivers, "dark kitchens" and couriers) will have to compete with each other for the best reputation and price within the platform.

The question is, of course, who will mainly benefit from the revenue generated within the ecosystem. Under the current circumstances, it is not inconceivable that for the next ten years, the major tech players will again profit the most from these developments, at the expense of local businesses and employees. Due to their dominance on all these layers of the Stack, they have managed to attain the extraordinary position of ecosystem orchestrator and thus rent seeker (think, for example, of Apple's App Store, Google's ad networks or Amazon's voice assistant Alexa). An important instrument in this is the collection of usage data, with which the user experience of these platforms and ecosystems can be further optimised, so that more users are drawn into the ecosystem, more suppliers join and more data can be collected again.

At the same time, we have established that, with new measures, governments are attempting to prevent the consolidation of large gatekeepers from creating an uneven playing field. If the European Union establishes legislation that promotes data sovereignty, data sharing, interoperability and open innovation, this will allow new data revenue models to arise, with which the service provider, but also citizens and companies will be able to profit from their data. In fact, a whole new generation of services could emerge that generates value based on the data previously trapped in the sealed silos of platforms. To facilitate this data sharing, there will also be a need for providers of data sharing services. The Netherlands might be able to repeat the success of AMS-IX here, by becoming, in addition to an internet exchange point, a data marketplace and hub for the data sharing economy.

The decentralisation of platforms through web 3.0 protocols and cryptocurrencies is a counter-movement that could further democratise earning capacity in a similar way. Citizens could become co-owners of the platform and profit from the value creation that takes place on it. In addition, tokenisation could help citizens to generate income in a low-threshold way by sharing their goods with others or making them investable. This would also enable them to trade in self-generated energy, digital content or data.



Theme 2: Public administration

Governments are using digital technology increasingly often by digitalising existing processes or innovating in the field of policy development, implementation, enforcement and participation. On the one hand, this provides opportunities for effective, efficient and just governance with democratic support, but on the other hand, it introduces risks such as rigid enforcement, weakened sovereignty and excessive focus on matters that are measurable and predictable.

The digitisation of public administration has long begun with the steady rise of digital government services. Similar to mega-ecosystems, the government will eventually interlink all its service counters through one user-friendly interface so as to stimulate adoption and citizen participation. Noteworthy - though not necessarily worthy of emulation - examples of this can already be found in countries such as Estonia, Taiwan and Singapore, where governmental and non-governmental services can easily interact digitally with government data.

Digitisation has also made its appearance in the domain of enforcement, with the use of scan cars to uphold parking policy, speed cameras, trajectory speed checks, security cameras and facial recognition technology at Schiphol Airport. However, the progressive sensorisation of our environment also raises the question of where and when such practices conflict with fundamental rights, especially in the context of government surveillance.

With the datafication of society, it is becoming possible to implement and enforce policy by means of ever more autonomous technologies. However, it is clear that there are limits to automation: the straightforwardness of code leaves no room for interpretation, reasonableness or fairness and the human dimension will come under pressure. While this may raise legitimate concerns about justice, disproportionate forms of control and risks of (inadvertently programmed) discrimination, it also creates opportunities for more just enforcement, as it makes decision-making transparent and allows human arbitrariness or prejudice to be consciously excluded.

On a higher level of abstraction, the use of digital technology could eventually lead to a shift from policy priorities to matters that are measurable and controllable. Matters that are not directly measurable, such as mental health or autonomy, could then fade into the background, while matters such as safety or physical wellbeing are placed higher on the agenda.

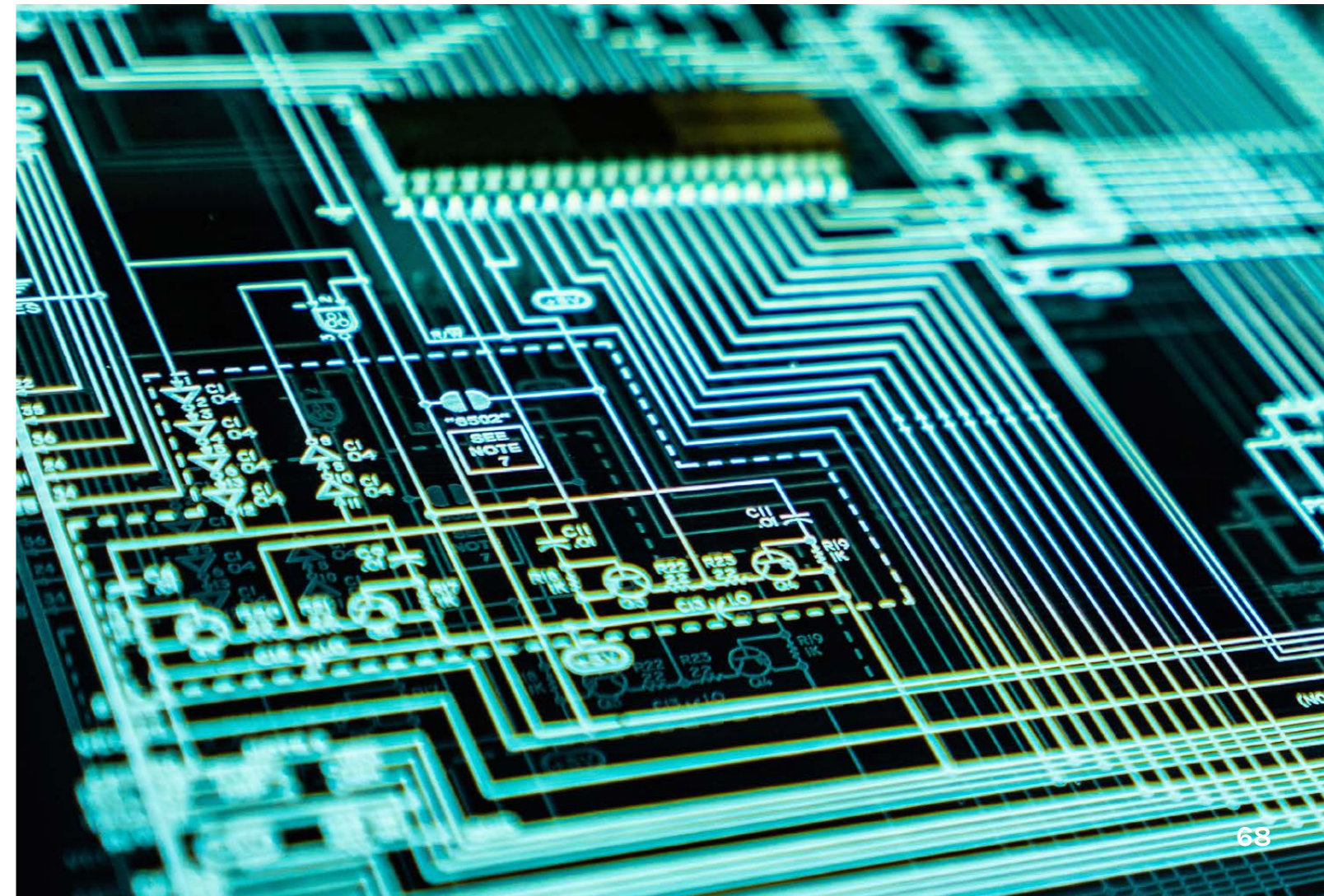
With regard to the development of new policy, digitalisation offers interesting opportunities as well. For citizens, codifying decision-making could lead to direct forms of participation, because it enables them to easily watch and participate in programming. Consider the institutional innovation that could arise if citizens worldwide collaborated on GitHub-like platforms and built an (international) library of open-source "smart laws".

We can also expect other forms of citizen participation and accountability. New forms of decentralised governance are already common within crypto networks: for example, users can vote "quadratically" on new protocol proposals based on their proportional contribution

to the network (determined via so-called "governance tokens"). Partly thanks to these types of possibilities, it is conceivable that initial resistance to automated governance will eventually soften and society will even be more open to strict enforcement of policy, as long as the code used is arrived at in a sound manner, with sufficient democratic support.

However, our growing dependence on technology may also put pressure on democratic support, as well as values such as sovereignty and responsibility. For instance, how will we deal with algorithms whose workings are not fully transparent to policy officers? And to what extent can governments make use of privately developed algorithms, when they cannot always be aware of the full array of their features, and which may make them too dependent on the developing parties?

To complicate matters even further, we are also seeing technologies emerge that place full control and autonomy with citizens, putting the position of governments under pressure, as is the case with, say, decentralised "self-sovereign identity" systems and data vaults. It is clear that digitalisation is leading to a fundamental reconsideration of the role of the government. This relates to its own hunger for data from and about citizens, but also to the way it manages and uses that data and, for example, allows it to be shared among different agencies. It is quite possible that, by way of the described technological means, citizens will gain a much stronger position in this respect and governments will no longer take up a central and dominant position.





Theme 3: Comprehensive wellbeing

Digitalisation could contribute to comprehensive wellbeing by supporting sustainable practices and making them more attractive, but also by enabling different forms of policy and introducing new rules of play to the economy. Potentially, digitalisation could also advance a higher quality of healthcare and education. An essential condition is that citizens must have equal opportunity in a digital society and that digitalisation does not lead to greater differences in prosperity and wellbeing.

Digitalisation can contribute directly to sustainability by, for example, making the energy system smarter or production processes more efficient. In addition, digitalisation is an important part of sustainable business models, in which coordination between different parties and processes is crucial. This applies to circular models, but also to sustainable as-a-service models (such as in the sharing economy) in which data and intelligence contribute to optimal balance of supply and demand and a good user experience. Technological developments have enabled simple data exchange between different services and links in value chains. This exchange can take place within closed ecosystems under the auspices of large tech companies or in a more open model in which independent parties exchange data with each other based on shared interests.

A smart economy is an economy that employs data to provide insight into problems relating to sustainability and inequality of opportunity and to develop policy accordingly. This also gives rise to the possibility to better quantify various negative externalities, such as environmental pollution or health damage and, if desired, to pass them on to the price of goods and services (so-called "true cost accounting"). In the long term, this could open the door to an entirely different model of taxation. Large-scale use of blockchain technology and smart contracts could even largely automate the settlement in the form of "micro taxing".

An important condition for this radical use of digital technology is that society actually has confidence in the technology and the intentions of the developers and managers. This requires transparency in technology, but also technology that does not lead to growing socio-economic inequality. To this end, it is very important that digitalisation benefits society as a whole and that everyone is able to take advantage of the opportunities offered and recognise risks. First of all, this requires basic digital skills, including literacy. New, intimate and more intuitive interfaces could be instrumental in this, because they are based more on (natural) speech and images than on written text, for example. However, this does not mean that everyone will be equally able to understand and, if desired, make optimal use of the new possibilities of advanced digital services, autonomous systems or cryptocurrencies. Initially, these options will mainly be available to the wealthy.

This is especially true of ways to "enhance" ourselves physically and cognitively with the help of new interfaces and digital assistants. Moreover, various initiatives to decentralise the Internet and the platforms operating on it in order to give back control (including over data) to users, will encounter a similar problem. In this case, too, additional skills will be needed, precisely because these are - by definition - systems in which central supervision is lacking. This offers opportunities, but may also lead to (security) risks.

The progressive transfer of old practices to the digital sphere and the development of entirely new practices also creates opportunities for the improvement of comprehensive wellbeing. To a certain extent, it still holds true that online, everyone is equal and able to shape their own identity. In the new virtual worlds, it is quite conceivable that everyone will have equal access to educational applications and that experiences will be within everyone's virtual reach. In practice, however, certain patterns may prove difficult to break: online gated communities will provide opportunities and protection that will not be accessible to everyone. In addition, platforms will consciously create scarcity and entice their users, by means of, say, expensive "skins" to convert their "physical wealth" into visible "online wealth".

Europe could fulfil the promise of comprehensive wellbeing through digitalisation by developing its own model of public-private collaboration. The first steps towards this have been taken with the European data and AI strategy, but other important measures that are underway are the strategic review of the ECB (e.g. including sustainability in risk analyses) and stricter laws and regulations (e.g. the mandatory "reparability" of goods). There is, however, a risk that more regulation will benefit large parties in particular, because they are better equipped to deal with it, and it raises barriers to market entry for new players. Moreover, the question is whether Europe will succeed in building a digital ecosystem of sufficient innovative power and scale to compete with the American and Chinese ecosystems. If so, the European model - followed by European companies - could gain a foothold in new markets that are also "stuck" between the Chinese and American Stack (e.g. India). The development of a Stack based on a European model would offer opportunities not only in regard to internal comprehensive wellbeing, but also to European earning capacity and geopolitical influence.



Theme 4: Security

Further digitalisation could contribute to our personal, national and economic security, but would also inevitably introduce a number of risks. These risks are linked to the degree to which our security depends on (foreign) companies, the rise of autonomous systems, and the increasing cyber-insecurity.

One question that arises when we look at the trends is what part the major technology companies will play in our (online) security. It is likely that, based on their expertise and financial prowess, they will be particularly suited to protect our data and systems against malicious parties. This could be an argument for investing our data and services with them rather than with smaller local companies or public platforms. At the same time, we are becoming increasingly dependent on these parties as their role in our daily lives and the economy grows. This makes us vulnerable to their potentially harmful intentions and willingness to protect their interests.

Alternatively, we could rely more on public or even fully distributed systems. The latter in particular have a number of fundamental advantages that would make this a feasible option. Centralised solutions always run the risk of a so-called single point of failure: a design flaw or vulnerability that can undermine the entire system or network. This is much less of a liability with a decentralised solution, because they consist of equal "nodes" that can take over each other's tasks when one of them (or more at the same time) experience(s) a problem. Because these systems are generally developed through an open source model, in which a large group of developers monitor and improve each other's work, allowing systems to evolve at a rapid pace, they are often more robust and resilient.

Another security issue relates to the development and embedding of autonomous systems. The advent of autonomous weapon systems and independently operating cyber weapons is especially concerning, but civil applications carry risks as well. First, because they can be hacked, so that autonomous vehicles (or digital implants), for example, can be manipulated. Second, an autonomously operating system can cause major damage when it makes wrong decisions due to technical problems. It will not always be clear how such a problem arose, whose fault it is and who is ultimately liable. It can have major consequences for citizens if they have trouble defending themselves (legally), against, say, a developer or government. The risks require technological guarantees and clear agreements and regulations. The first steps towards this have been taken, but societal discourse about the role of autonomous systems has yet to take place.

There is no clear-cut solution that addresses the various threats and risks associated with the digital transition. Technological solutions will be part of the answer: this means more stringent security measures and expansion of cybersecurity expertise, with regard to the vulnerability of existing security systems to quantum computers, for instance. Other examples are systems that enable citizens to better defend themselves against data-hungry platforms, and the building in of a (human) control function to overrule or disable autonomous systems when necessary. Another part of the answer is the commitment of society, which is necessary for the

technological solutions to be effective. In the future, cybersecurity will (still) mainly be a shared responsibility between developers and users of systems. Companies and governments will have to be more aware than they have so far been of threats and citizens will also have to (learn to) arm themselves better against risks.

Finally, we cannot separate security risks from the geopolitical battle that is also manifesting itself online: in the form of espionage and sabotage, but also in negotiations about new technological standards. The next generation of key technologies (such as quantum computers, AI and biotechnology) is pre-eminently dual-use in nature and the distinction between civil and military applications will be increasingly difficult to make. This will lead to new technology raising ethical, economic and strategic questions.

An important consideration will be which technology a society should develop (and produce) itself and with whom that technology will be shared. Another question is whether we will continue to adhere to the ideal of the worldwide web in the future. It is still unthinkable as yet, but security considerations may prompt us to (partially) disconnect our Dutch and European Stack from the Stacks of other countries. In part, this is already happening with the storage of data, but in the future it may also apply to services such as social media or payment transactions.



5

Theme 5: Public values

The trends described are not unequivocal in terms of public values. Digitalisation may help strengthen and deepen our democracy, new technologies could allow us to recover our online privacy and autonomy and technology can have a moralising effect in a positive sense. At the same time, the online ecosystems of the future could contribute to a deep fragmentation of society, in which case the question will be who sets and enforces the rules within an ecosystem.

In the coming years, the formation of social bubbles may lead to further polarisation and online fragmentation, whereby groups do not merely use their own favourite platforms, but also their own cloud services and operating systems. In this case, people with differing views will no longer come into contact with each other, there will hardly be any correction of fake news and the idea of a shared reality will disappear altogether. This effect could spread to virtual worlds, where groups can shape their own reality and the difference between real and fake is even less meaningful than on today's social media. As discussed above, these online worlds may either take on a global character with cross-border norms and values, or they will be rooted in local communities and the prevailing ideas there.

In these virtual environments, it will primarily be developers who determine and enforce the rules. On which values they will be based remains to be seen: the values of the country of origin, the values of (some of) the users or perhaps of the developers themselves? In any case, odds are slim that governments will have any (or much) say in this. It is already proving virtually impossible for governments to get a grip on digital platforms. This will only become more challenging with the increasing complexity of systems and the growing role these platforms play in our daily lives.

None of this alters the fact that the digital transition can also be used to combat existing abuses or misconduct. For example, data can help to provide insight into certain matters (such as inequality of opportunity) and advanced models can help to design and simulate solutions. Going one step further, algorithms and autonomous systems can expressly be used to eradicate existing abuses or to enforce moral behaviour on the part of users. For instance, a robot taxi will not refuse people based on the colour of their skin colour and can be programmed in such a way that unwanted behaviour (such as speeding) is simply impossible. Such forms of "moral unburdening" undoubtedly offer many (measurable) benefits in the way of safety (and possibly sustainability), but also raise the question what will remain of our autonomy if we continue to gradually outsource it to technology.

While on the one hand, we are at risk of losing autonomy, we may be able to regain autonomy in other areas. If, in the future, citizens have access to a personal data vault, they will be able to manage their own data and freely switch platforms. Ideally, data sovereignty would also encourage the sharing of data for the common good, for research or for establishing public facilities. In this scenario, much of our online practices could take place in a public space as opposed to the private space where they take place now, and governments could again be tasked with managing this public space.



Chapter

6



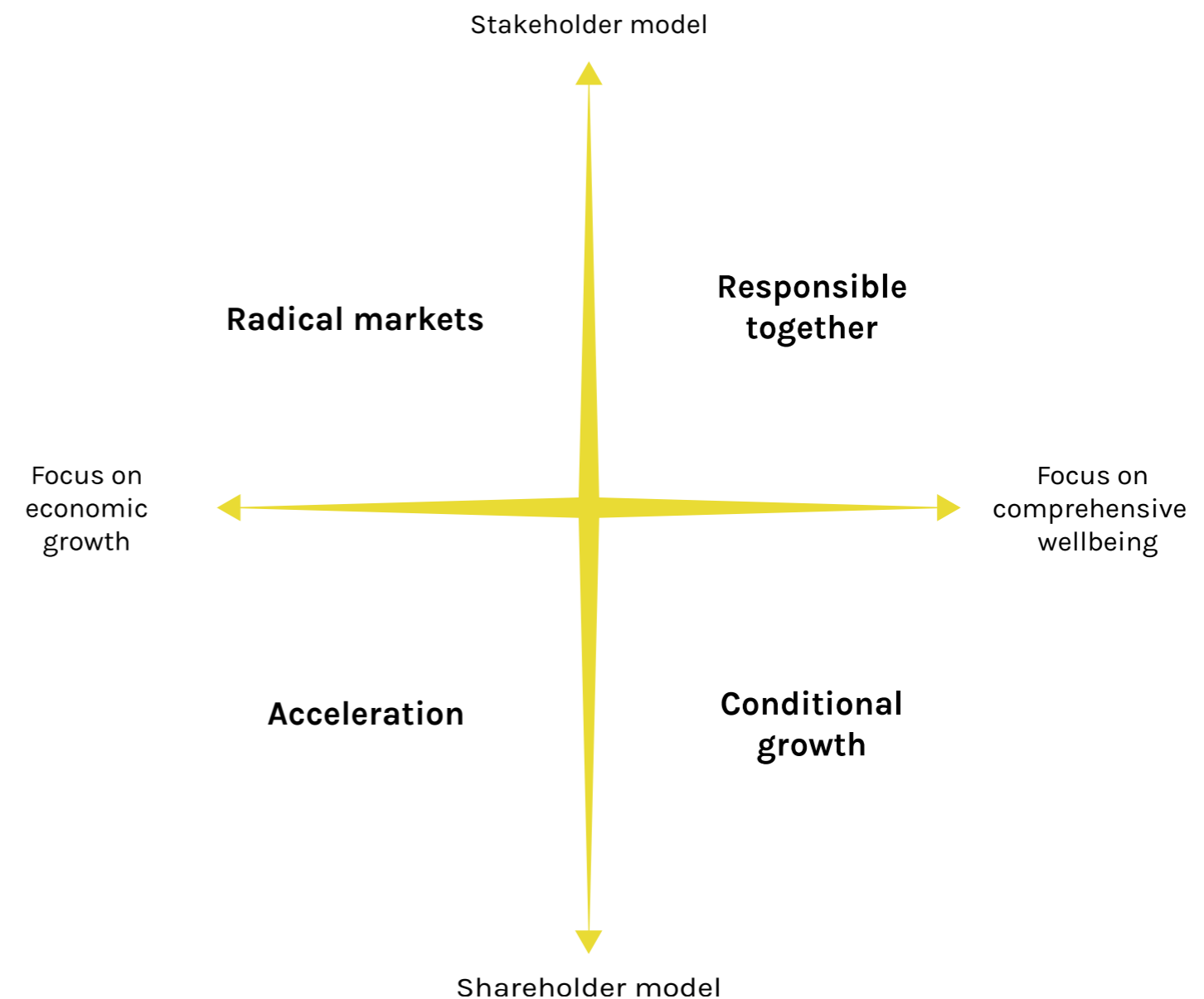
Scenarios for the future

The trends and the analysis of the possible consequences of digitalisation do not provide a clear image of our digital future. This has everything to do with the fact that every trend is subject to many uncertainties and that several divergent development paths are conceivable. Nevertheless, the trends do make us aware of the most important themes and questions to which society, and therefore the government, must formulate an answer. Here, we incorporate the possible answers to these questions, and underlying uncertainties, in four different scenarios for the future, on the basis of which we can explore the desirability and feasibility of different options.

Two of the most important questions relate, respectively, to the leading actors in the digital transition and the goals that we hope to achieve through digitalisation. The first question particularly aligns with concerns that are already relevant today in regard to the dominant position of a small number of (non-Dutch and non-European) technology companies. If this does not change in the coming years, the question arises what this will mean for the earning capacity of the Dutch (and European) economy, but also who will determine the rules of play for the digital world. The second question is closely linked to this and pertains to the role of digitalisation and the possibilities it offers for realising societal ambitions with regard to equality of opportunity and sustainability.

We can use these key questions to think about our digital future in a structured way. We do this by means of four scenarios for the future in which society deals with these questions and the underlying challenges in different ways. In these scenarios, we sketch worlds in which either (the current) private platforms are dominant, or alternative, more public platforms replace them. This distinction relates to the difference between a digital transition based on a shareholder model or on a broader stakeholder model. With regard to the goal of digitalisation, we differentiate between scenarios in which digitalisation is explicitly used to achieve comprehensive wellbeing and scenarios in which economic development is paramount.

The four scenarios for the future that result from this are magnifications of (future) reality, which help us think about the advantages and disadvantages of various answers to the major questions surrounding digitalisation. They thus form the first step in a process of "backcasting", in which we can ask ourselves which scenario for the future of digitalisation is most desirable and which steps we can take to realise it. The scenarios below are meant to serve as inspiration and a starting point for dialogue. It is very likely that the most desirable scenario for the future will ultimately consist of a combination of elements from different scenarios. Obviously, we do not intend to fully predict the future and many questions remain to which these scenarios for the future do not provide an answer.





Future scenario 1: Acceleration

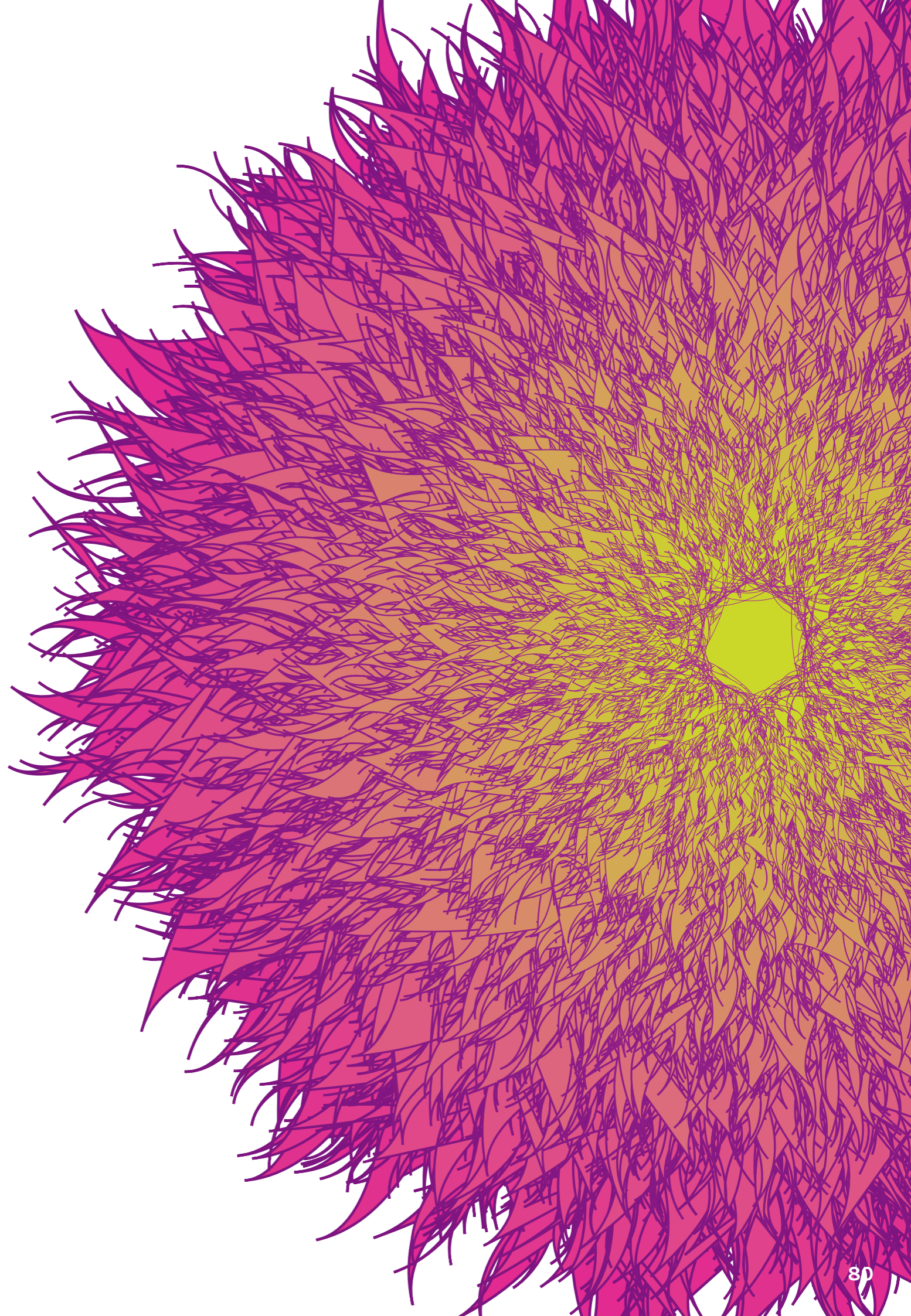
The digital infrastructure and main platforms are still in the hands of the major international technology companies, but the industry has shown a capacity to correct itself. Under pressure from employees, service providers and users, they have become more reticent with respect to collecting data and have become more transparent about their algorithms. They have thus managed to stay ahead of the call for stricter regulation and prevent alternative platforms, which are based on cooperation, from infringing on their position.

The services they provide within their integrated ecosystems are so appealing to users that the call for public or decentralised alternatives is being silenced. The same applies to providers of services such as shops, hotels and car rental companies, but also to professionals and aspiring "influencers".

Although they are obliged to pay the ecosystem part of their revenue, they get a lot in return: access to a huge market, extensive possibilities to link their own services to those of others, and analyses and insights based on data and intelligence, which they lack the competences to acquire themselves. This allows them to fully focus on matters at which they do excel.

Although these ecosystems partly come at the expense of Dutch activity, the platforms are indeed responsible for a large part of the economic recovery since the crisis and are, to a significant extent, directly and indirectly responsible for job growth. They are also an essential part of our security shield against hackers and enemy states. Thanks to their scale and unparalleled expertise, they are uniquely able to identify vulnerabilities and fend off attacks.

The power of digitalisation is thus used to achieve economic growth and to make life a lot more pleasant for (the majority of) the population. However, political agreement on the use of digital technology to promote comprehensive wellbeing is absent. Political debate remains stagnant due to disparate ambitions with regard to greening and equal opportunity, so that there is a lack of support for mission-oriented innovation and accompanying policy. Governments therefore limit themselves to "neutral" enabling policy that is primarily aimed at the construction of the digital infrastructure, the quality of (future-proof) education and cybersecurity.





Future scenario 2: Conditional growth

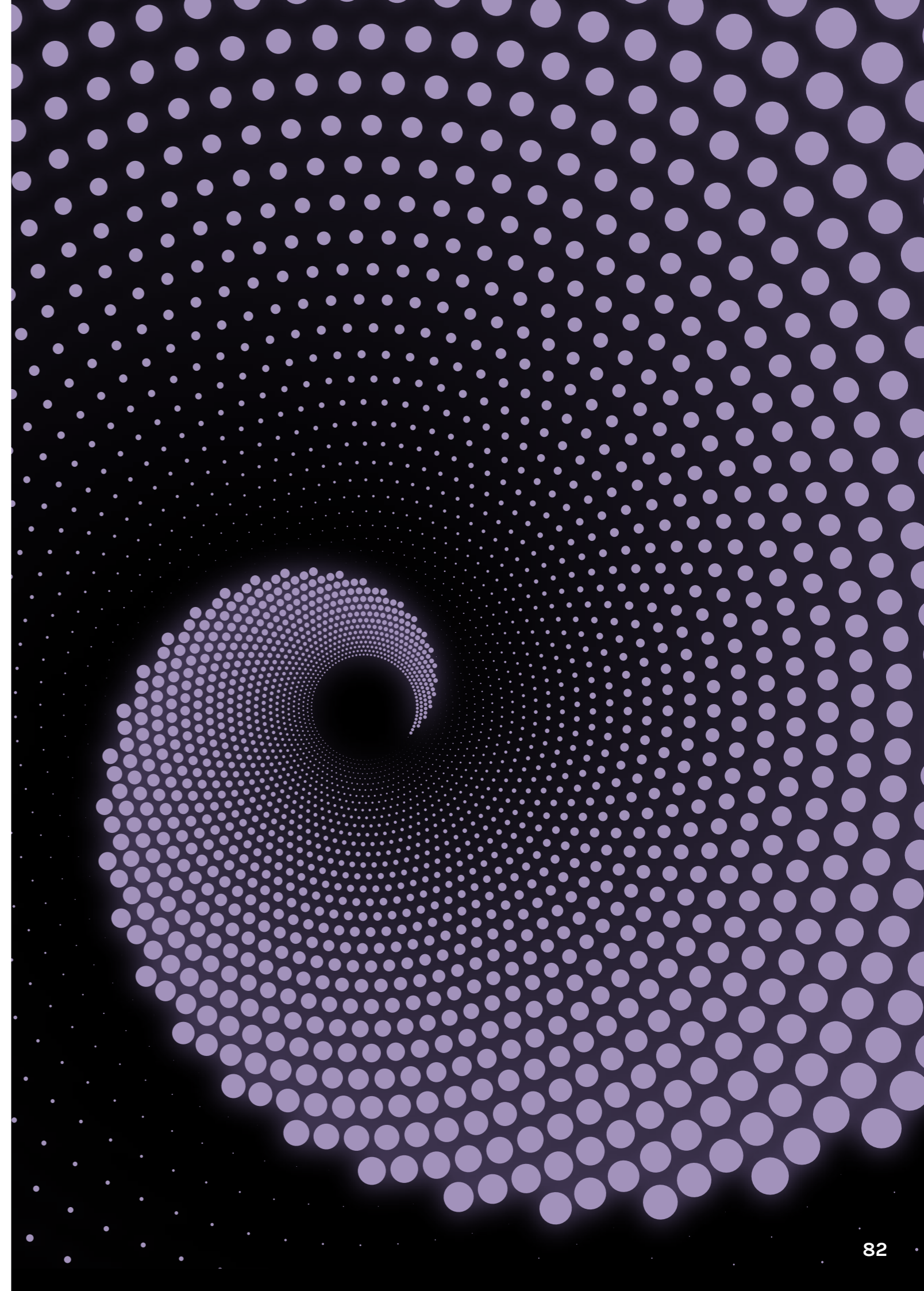
The internet as an unregulated free state ceases to exist. It did not work for its users, had negative effects on society and compromised the Dutch and European earning capacity. Europe has therefore proceeded to implement more stringent regulation in regard to online activities and the platforms on which they occur. These regulations pertain to the handling of data and the use of algorithms, but also specifically to the impact of digitalisation on our living environment and ourselves.

Although the unprecedented market power of the large platforms provided many free or cheap services for end users, they came at the expense of suppliers, who were pitted against each other. The end users themselves became increasingly trapped in the web of the big tech companies and gave up more and more of their online freedoms. Initially, the solution is sought in co-regulation between the sector and governments, but this does not lead to the desired results. Society calls for strict top-down regulation as the logical response. Naturally, it is feared that this means Europe is sidelining itself and that large companies will avoid the Union. Others fear that European companies and citizens will not be able to use services of the same quality as the U.S. and China because of this policy.

However, the key to success appears to be the gradual implementation of regulations with a clear multi-year plan. This means that the technology companies are perfectly able to develop further, both technologically and economically, and to meet the demands of society. At the same time, governments, in collaboration with the European scientific community, manage to develop their own competences to be able to carry out checks in a meaningful way.

Data portability is crucial to safeguarding the online freedom of citizens. Plans to let users manage and trade their data themselves have previously failed. Too few people felt compelled to invest time and energy in this and not everyone was able to make wise choices, which meant that exploitation and abuse were all too common. The responsibility for data has therefore been placed with the business community, on the condition that citizens can always take their data with them to another ecosystem if they want to switch. The result is a digital world in which business no longer "reigns", but in which the power of the market and the innovative capacity of companies are used to enable digitalisation to benefit society as a whole. The rise in comprehensive wellbeing can largely be attributed to the highly accessible services of these companies. Solutions such as mobility-as-a-service, as well as innovations in education, healthcare and safety, contribute to this and, thanks to strict policy, they are actually accessible to the masses.

The old adage that the online world should have the same rules as the physical world, has been abandoned. Because misconduct in the digital sphere, due to scalability and rapid distribution through the network, can have particularly far-reaching consequences, governments in fact impose extra strict rules on the virtual world. The emphasis here is on inclusivity and rules of play that finally make the virtual world the "safe space" it was always meant to be.





Future scenario 3: Radical markets

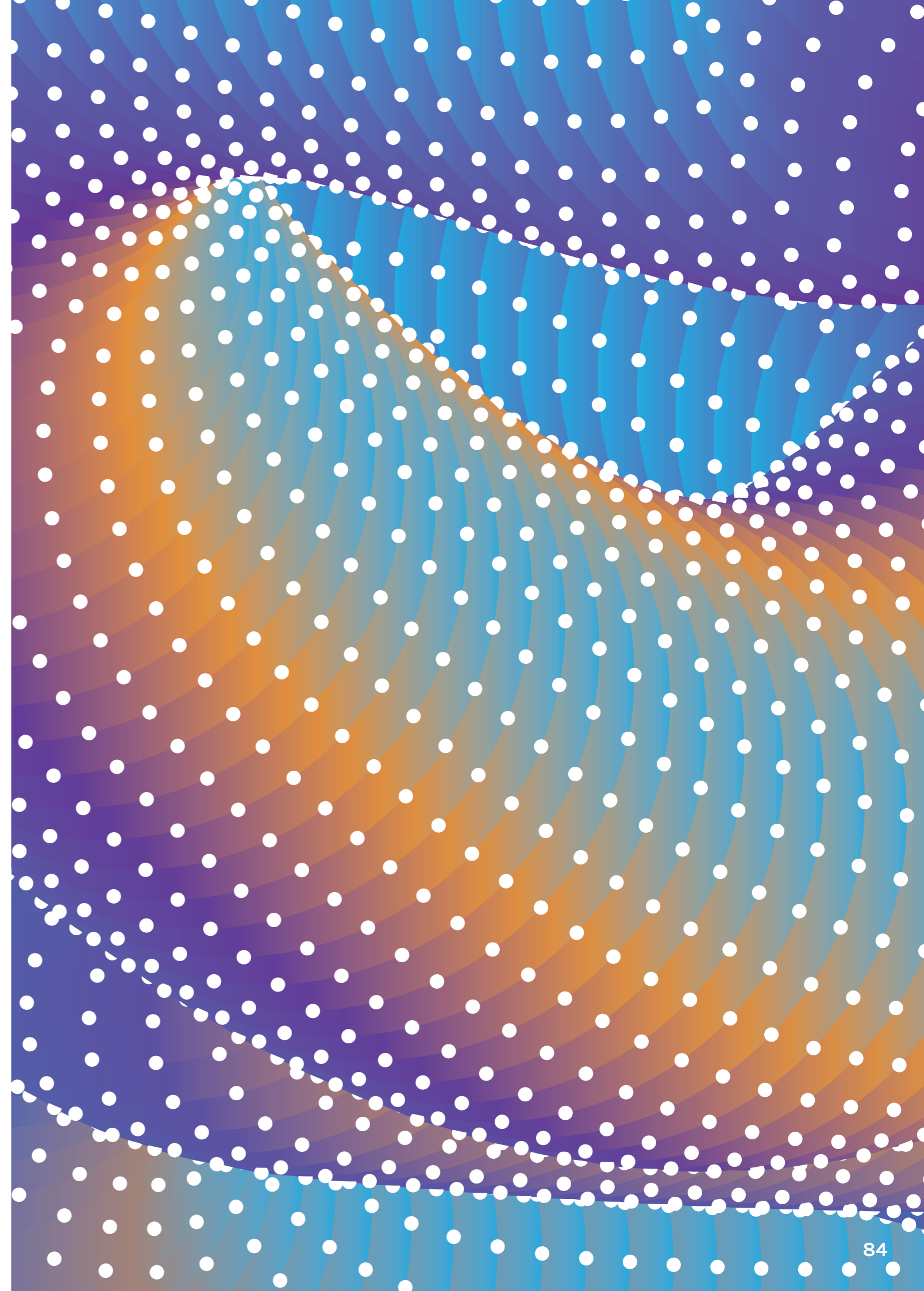
It was the market that produced the tech giants and it is the market that seems to be dismantling them. Critics agreed that the power of Big Tech was difficult to break and that only drastic government intervention could remedy this. The real solution, however, comes as a surprise. Whereas the rise of cryptocurrencies was initially seen as a speculative bubble, in hindsight, it can be said to have been a public capital injection to develop a new Stack, also known as web 3.0.

Basic functions such as digital financial transactions, self-sovereign digital identity, personal data sovereignty, privacy and data sharing can be made available through this open-source infrastructure as a kind of utility. All without the mediation of a central party. Many of the principles of web 3.0 appear to be in line with the new European measures for a common digital market. This means that the so-called Brussels effect also boosts the adoption of this new generation of internet protocols outside of Europe. On this web 3.0, we see the gradual emergence of an integrated ecosystem of both local and non-local decentralised alternatives to Google, Facebook and Amazon. The main difference with these predecessors is that the new platforms and the data and algorithms generated on them are in the hands of open stakeholder networks, in which end users, developers, service providers and network validators jointly determine the rules.

Disproportionate service fees and unequal distribution of created value are thus a thing of the past. We even see services on offer that would probably not have been able to exist in the old platform economy, such as cross-sectoral "smart city" solutions. The combination of data-driven transparency, open innovation and a network-driven stakeholder model means that markets are better able to respond to the "long tail" of social needs.

Yet, comprehensive wellbeing is not a self-evident consequence of the web 3.0 society. Its decentralised nature also leaves room for undesirable practices such as market manipulation, illegal trade and the distribution of illegal and hateful content. In some networks, anonymity also leads to political manipulation of the stakeholder model. The biggest challenge lies in the fact that these networks do not care about national borders and (national) governments do not have any control over them.

This means that governments are unable to protect their citizens online, but also that they have virtually no say in the type of solutions that are developed and their impact on society. In this way, the range of duties performed by governments gradually dwindles. The question arises whether, and if so, how governments can appropriate a role for themselves in these networks and be a part of, and thus have some control over, the development of this radically democratic model.





Future scenario 4: Responsible together

The hope that the digital transition would automatically lead to societal progress and a rise in comprehensive wellbeing has given way to a more realistic perspective. The Internet after the American model has mostly led to undesirable forms of hypercapitalism, growing socio-political alienation and cultural displeasure. In order to solve these problems and ensure digitalisation benefits society as a whole, Europe opts for the development of its own Stack, in which public-private collaboration is a central objective.

The intensive cooperation of governments and (European) business is partly prompted by their common interest in combatting the foreign technology giants. Using this renewed multi-stakeholder model, they work together on innovation and new platforms and services. This approach has also been facilitated by technological innovation that enables a less centrally orchestrated Internet, in which open data contributes to a fairer and innovative market. Openness and transparency ensure that public-private initiatives and their solutions can be scaled up more quickly (internationally). In this way, this typically European model fulfils the promise of network effects and the infinite scalability of digitalisation.

In the new structure, technological innovation goes hand in hand with social, economic and institutional innovation. Climate change is first on the agenda. Data and AI help to make systems more efficient, but there are also strict requirements for consumption and production. Digital systems, including means such as "carbon credits" and real-time supervision, ensure the acceleration of sectoral transitions. Initially, autonomisation and digital ecosystems have a negative effect on employment, but other jobs are created and a specific capital tax (the so-called "robot tax") and alternative revenue models enable citizens to contribute to society and the economy. A greater sense of morality and the increased self-awareness of citizens and consumers put pressure on companies to not only operate in a sustainable, fair and egalitarian manner, but also to internalise the perspective of society and to pursue well-being in a broader sense. Companies do not merely facilitate consumerism but also contribute to public goals and socially accepted innovations.

The government plays an active role by weighing up the advantages and disadvantages of the centralisation and decentralisation of different layers of the Stack, taking account of the different interests in the multi-stakeholder model and developing open and transparent policy-making processes, in which every citizen, producer, consumer and prosumer can participate. This unique course also requires Europe to safeguard its own online security. Governments play a major role in this as well, by increasing digital awareness among citizens and businesses, but mainly by taking the lead in the development of cyber security as well as offensive capability. In a broad sense, this active role of the government also requires a new job profile for the policymaker. Knowledge of digital innovation will be a prerequisite for tackling the complex challenges of tomorrow while understanding and connecting the interests of different stakeholders.

Chapter

7



Final remarks

In order to get a grip on the digital transition, it is crucial to look as well as think ahead. This means that we must develop an understanding of technological possibilities, but also of the driving forces behind the development and deployment of this technology and the way technology and society shape each other. Based on the Stack framework, we have attempted to map out our digital future in this outlook. This has resulted in eleven trends in which technological developments converge with societal (counter)movements. Despite all the internal uncertainties, the trends show that there is still a lot to be done, both in terms of further development of existing technologies, practices and solutions to problems and in terms of truly new developments. Subsequently, we have attempted to speculate about possible scenarios with regard to the trends and the most relevant consequences.

When looking this far ahead by means of trends and scenarios, fundamentally different questions arise than when we only look a few years ahead. For example, we are forced to ask ourselves the question who should be responsible for the digital infrastructure and the most important platforms and ecosystems in the longer term. A traditional, old-fashioned government, a new international entity, or would a radically democratic system within a decentralised governance model also be a possibility? We are not asking this question because of short-term concerns about privacy scandals, fake news or hate speech, but because we realise that digital ecosystems and virtual living worlds will come to play such a significant role in our lives that the rules that apply there will have a fundamentally different meaning than the terms of use or rules of play of the current platforms.

In a broader sense, a long-term perspective helps us realise that we have to make choices today, so we can shape and direct our digital future. If we fail to do so, we risk passively undergoing the digital transition, having choices made for us, incurring economic and strategic risks, and there is a good chance that we will be stuck with technology that does not accord with our values and standards. Making those necessary choices starts with imagining desirable, and realistic, futures. Then, we can ask ourselves how we can shape that future and what moments of choice lie ahead.

Of course, this is easier said than done. It requires society to be willing and able to think about technological and institutional innovation in a meaningful way. It also calls for a government that is prepared to make choices about regulation as well as the technology itself. After all, we have seen that technology is not merely a neutral means and that, as a society, we should be able to take part in decision-making about the design of sometimes self-willed, intrusive and invasive technologies. This may also mean that governments must more actively promote the development of (alternative) solutions.

It may even demand a government that, if necessary, is willing and able to take the lead (again) in the development and management of such systems. At present, the debate about digitalisation is mainly taking place in Europe, between experts and activists. Fundamental choices with

regard to digitalisation, however, also require a broad national debate. We sincerely hope that this outlook can contribute to this, either by proposing possible solutions or by providing inspiration for everyone who wants to participate in reflecting on our digital future.



Deep Dive:

building blocks of the digital transition

In this Deep Dive, we discuss the most important technological developments, per layer of the Stack, with 2030 in mind. Based on literature and discussions with experts, we make an estimate of what will be technologically feasible, which possible solutions are being explored and, partly, what this will mean in relation to other layers of the Stack. Where relevant, we also look briefly ahead at the interplay between technology and society. We limit ourselves here to the eight layers that are mainly technological in nature.

This overview of technologies is not exhaustive and explicitly formulating technological expectations is intrinsically challenging. Nevertheless, we aim to provide the interested reader with additional knowledge, as a background to the described trends, but above all as a basis for further exploration of ideas.

1. Resources

The recycling of resources and the use of less scarce or environmentally harmful materials are making the Stack more sustainable, just and less dependent on foreign suppliers.

Resources

At the bottom of the stack, efforts are being made to make the digital infrastructure more sustainable. Digital systems are partly made up of scarce resources, such as cobalt, indium and various rare earth metals, which are extracted under poor working conditions, with harmful consequences for the environment. Improper processing of these substances is also likely to harm the environment. Moreover, there is a worldwide scarcity (of so-called conflict minerals⁴) and production often rests with China, which regularly threatens export restrictions. In view of the specific requirements, alternative materials will not be feasible in the coming years. The (Western) world is working on a solution in two ways. On the one hand, countries are investing in their own production (e.g. the U.S. is restarting domestic production, after it ceased to be considered profitable decades ago) and searching for minerals in other, politically stable, countries. On the other hand, they are working hard to establish methods of refining the recycling of materials and also to recover minimal fractions of materials from electronic waste.⁵ This applies specifically to li-ion batteries, from telephones, laptops and electric vehicles, from which, in addition to the main component lithium, cobalt must be recovered. The same is true of metals such as indium, of which far more could be recovered than is presently the case.

Energy consumption

The other major concern regarding digitalisation and sustainability is the rapidly increasing energy consumption of the global Stack. In the Netherlands, the electricity consumption of data centres increased 66% in two years, so that in 2019 these bulk users already accounted for 2.7% of the total electricity supplied by the public grid.⁶ Without advancements in energy efficiency, the energy demand of the use of ICT worldwide will increase to more than 20% of the total energy demand, largely because of datacentres and networks.⁷

2. Hard infrastructure

The costs of hardware continue to drop exponentially and new technologies offer the necessary computing power and connectivity for artificial intelligence applications and the next generation of digital services. The advent of quantum computers is leading to breakthroughs in specific tasks such as modelling and searching large amounts of data.

Conventional computing power

In recent decades, the number of transistors per chip has doubled every two years. However, the current path of development, based on progressive miniaturisation, is in danger of stalling by 2025.⁸ The exponential decline in computing costs will continue in the coming years, but with the ever-improving performance of chips, the end of Moore's Law seems to be in sight. Radically new concepts are being developed, but they will not yet see a breakthrough in the coming decade.

In the coming years, however, much more is expected from further specialisation of processors based on existing technology. Specific hardware, so-called accelerators, will enable certain tasks to be performed much more efficiently than with traditional general purpose processors. This is especially true for graphics applications (e.g. in gaming) and for the development of artificial intelligence applications. Such specialised hardware is already in use now, but it is expected that the trend of specialisation will continue and that the chips of the future will contain a large number of this type of (stacked) modules. The development and application of this specialist hardware goes hand in hand with the development of new software (algorithms) that make optimal use of the possibilities of, and ensure cooperation between, the different modules.

The costs of this kind of highly specialised hardware-software combinations are higher than those of traditional generic processors (all-rounders) and this could hamper further innovation (especially for smaller system developers).

Due, in part, to this, developers are supportive of the emerging open-source hardware movement. Most striking is the development of the RISC-V standard for chip design.⁹ Apart from the specific design advantages, the open source approach in hardware could lead to better interoperability between systems and lower development costs, thus increasing the chances of new entrants to the market.

Quantum computers

In addition to the further development of conventional computing power, we will also see the first practical applications of quantum computers in the coming ten years. The workings of quantum computers are incomparable to those of conventional processors and it cannot be taken for granted that they will replace the traditional computer. Initially, they will only be used by institutional users, scientists and the business community, to solve highly complex and specific problems. In that sense, the quantum computer will, for the time being, be on par with the large mainframes from the beginning of the computer age. At the moment, a number of parties (Google¹⁰ and a Chinese University¹¹) claim to have achieved so-called quantum supremacy; the ability to perform a calculation that is practically impossible for a conventional (super)computer. However, this does not mean that these computers will be of immediate value. The computing power of quantum computers is often indicated by the number of so-called

qubits with which they perform calculations. At the moment, we are dealing with "only" dozens of qubits, but IBM claims to be working towards hundreds of qubits per system in the coming years and hopes to be able to build systems with over a million qubits by the end of the decade. In addition to this exponential increase in computing power, the reliability of calculations is also supposed to increase.¹²

The special properties of quantum computers could make them particularly suitable for solving specific problems, such as optimisation problems, search problems and especially modelling (the behaviour of) atoms and molecules. The latter creates high expectations for quantum computation in, for example, drug development and the development of new materials (e.g. batteries). A major concern is that quantum computers will be able to decrypt existing forms of encryption. On the one hand, this means that existing security systems will have to become stronger in the coming years (or otherwise less vulnerable to this threat). On the other hand, it also means that enormous amounts of encrypted data already in the hands of intelligence services, for example, will soon become readable.

Edge and fog computing

In recent years, a lot of data and computing power have been joined in large data centres (the cloud). This has the advantage that costs for users have been reduced (due to lower hardware and maintenance costs) and that services have become more reliable, more easily scalable and better secured. More recently, we have also been seeing a trend that restores data storage and computing power to the end user; edge and fog computing. Whereas edge computing refers to data storage and computing power in devices at the extreme edge of the network (such as a smartphones or sensors), fog computing refers to an intermediate form, in which, for instance, a local server (sometimes called a cloudlet) collects and processes data from different devices or sensors.

The rise of edge and fog computing is driven by the need to minimise time losses due to data transport (e.g. for critical real-time services), to reduce costs and risks of data transmission, and to combine and make optimal use of the computing power of many small devices.¹³ Moreover, this kind of distributed model of data storage and processing is essentially more robust than a central model in which, theoretically, a single error could paralyse an entire system. Finally, decentralised data storage and processing also offer the advantage that control over (and possibly insight into) data is limited to several smaller and therefore less powerful players.

5G and other network technology

In the coming years, the 5G network in the Netherlands will be expanded and additional frequency bands will be issued. It is expected that 5G will be available throughout the Netherlands by 2025.¹⁴ This is in line with the European ambition of 5G availability by 2025, in all urban areas and along transport corridors.¹⁵

Lower costs, higher speed and minimal delay have already made new applications and services possible. The main challenge for the next ten years will be the construction of infrastructure, the development of new services and the adaptation of existing devices, systems and (consumer) practices. Consumers will mainly use 5G for entertainment (such as gaming and video streaming). In addition, 5G will be pivotal in the development of autonomous transport systems; of passenger transport, but also public and freight transport). 5G will also contribute

to the further development of e-health and making industrial processes smarter, more efficient and safer.¹⁶ The logical successor to the 5G standard, 6G, will not come into view before 2030.

Besides the development of the 5G network, we are also seeing the emergence of low-orbit satellites for communication in remote areas and extremely energy-efficient connections (so-called low-power wide-area technology such as LoRa¹⁷) for small devices and sensors for the "Internet of Things".¹⁸

3. Soft infrastructure

The costs of hardware continue to drop exponentially and new technologies offer the necessary computing power and connectivity for artificial intelligence applications and the next generation of digital services. The advent of quantum computers is leading to breakthroughs in specific tasks such as modelling and searching large amounts of data.

If we were to look behind the scenes of the applications we use every day, we would see that they consist of various modular software building blocks. Each of these building blocks fulfils an important function such as controlling, connecting and virtualising hardware (e.g. firmware, network protocols, kernels/operating systems and middleware), managing databases, organising the business logic or the way information is ultimately presented to the user (presentation layer or front-end).

However, because these building blocks form the foundation of entire software ecosystems, the administrative frameworks with regard to interoperability, data sovereignty, privacy and open innovation, are also determined here. From this point of view, we will take a closer look at a few interesting developments.

Blockchain

A blockchain is essentially a distributed database that allows participants in a network to share and independently verify data without the intervention of a central intermediary. Instead, a so-called consensus protocol is used, in which game-theoretical principles are applied to allow the entire network of actors to contribute to updating and securing the network. This results in a federated infrastructure where both the data and the data platform itself are not owned by one actor, but by the entire network of stakeholders. Blockchain was first applied with Bitcoin, but variants are now used with all kinds of other cryptocurrencies and federated applications.

Blockchains come in "permissioned" and "permissionless" varieties. Permissioned blockchains work through authorised nodes, meaning a consortium of stakeholders authorises new entrants to the network. Permissionless blockchains, on the other hand, do not have an authorisation process for new nodes. Instead, open consensus protocols are used (e.g. proof-of-work, proof-of-stake, delegated-proof-of-work), in which network validators are stimulated with codified economic reward structures or punitive cryptocurrency measures. With permissionless blockchains then, cryptocurrencies are not merely an application of blockchain technology, but also an important technical element to keeping the network safe.

Due to this technical aspect, permissionless blockchains still contend with the so-called blockchain trilemma, in which a trade-off has to be made between the degree

of decentralisation, scale and security. For example, the bitcoin blockchain currently only offers a transaction density of approximately seven transactions per second. With a store of value function in mind, bitcoin has deliberately opted for a high degree of decentralisation and network security, while scaling the transaction density is less of a priority.

In this, we see other cryptocurrencies making different protocol choices in the trade-off between these variables, depending on the functionality that these blockchains want to offer the applications that are built on them. In addition to the blockchain trilemma, other issues such as privacy, energy consumption, openness, interoperability, transaction costs and governance are also considered in the design of the protocol. Moreover, as with the design of the Internet, according to the end-to-end principle, not everything will be addressed in the main protocol, but rather in the higher protocol layers (second-, third-layer solutions). For example, we see that there are second-layer projects aimed at tackling the transaction density and high transaction costs of cryptocurrencies by storing transactions in the blockchain in groups.

Permissioned blockchains in turn generally opt for scalability, at the expense of decentralisation and openness. As a result, permissioned variants will mainly play a role in smaller consortia, in which stakeholders already trust each other. However, when it comes to developing a global internet infrastructure, permissionless variants in which decentralisation and open innovation tend to be maximised will probably be the preferred choice, as they have been in the past.

Privacy-preserving technology

Decentralising data infrastructure appears to be a possible solution to concentration of power, but it will not solve privacy problems. To that end, a lot of work has been done recently on cryptographic schemes, which should help accord web 3.0 privacy by design. This includes solutions such as homomorphic encryption, secure multiparty computation and differential privacy.

Homomorphic encryption is a cryptographic scheme that allows calculations to be performed on encrypted data. Normally, this would yield unusable results, but with homomorphic encryption the computation is as good as if it were done on unencrypted data. The technology allows calculations on sensitive data to be outsourced to parties we do not necessarily trust. Consider, for example, offering recommendations based on your search preferences or making diagnoses based on healthcare data. However, homomorphic encryption is currently still facing scalability problems. For instance, calculations on homomorphic encrypted data are still very slow, which means applying the technique is not yet profitable for many applications.

Secure multi-party computation is another privacy-preserving technique with which calculations can be performed on the secret data of various parties. In addition to the results, the input data of the parties involved remains encrypted to each other party. This makes it more attractive for parties to share datasets with each other for the purpose of creating shared value. Consider, for example, the sharing of business-sensitive data within value chains for the purpose of increasing overall efficiency.

Hybrid & Multi-cloud

Now that the migration of large companies to the cloud is well underway, we can see that the emphasis on cost-efficiency and performance has gradually shifted to other critical requirements such as interoperability, data portability, anti-vendor lock-in and security. To achieve these goals, the cloud industry appears to be focusing on enabling companies to distribute their workloads across multiple computing environments, whether private and public clouds (hybrid cloud) or multiple public clouds (multi-cloud).

An important partial solution in creating these infra-agnostic applications is the use of containers. Containers allow for the quick and easy implementation of discrete application components that can be run in practically any cloud environment. That this solution is becoming more popular can be deduced from the growing number of companies involved in different parts of the containerisation value chain, be they container operating systems, container engines (e.g. Docker), container orchestration tools (e.g. Kubernetes) or application support services. Interestingly, many of these companies use open source code in some way, so that open standards can be easily formed with interoperability purposes in mind.

4. Data

The amount of data available is increasing because of our use of digital services and the addition of sensors to our living environment. This data offers real-time insight into behaviour, objects and processes and creates possibilities for governance. At the same time, it raises the question which problems this data should and can solve.

New sources of data

Data is the most important resource of the digital economy and will continue to grow significantly over the next decade. From 49 billion zettabytes in 2019, the global datasphere will expand to 175 zettabytes in 2025. Processing and storing these growing datasets is a challenge for companies and institutions. Most data will therefore be managed in the cloud.¹⁹

The datasets of the future will increasingly be linked to so-called data lakes in which unstructured data from a growing number of sources comes together. The largest new source of data is the Internet of Things (IoT), which comprises billions of small and large devices that will be connected to each other in the coming years. In addition to big data, we will therefore increasingly be dealing with "fast data".²⁰ Fast data is processed immediately and thus creates real-time interaction between governments, companies and customers or citizens. While big data is historically oriented and mainly revolves around generating knowledge from large volumes of data, fast data is more contextual and purposive.

This offers new possibilities for monitoring and modelling systems or processes and automating decision-making. An example of this is the permanent recalculation of optimal driving routes based on real-time traffic data. Increasingly, communication will not go through us, but devices will communicate with each other in real time, in which 5G will be an important facet. Consider, say, self-driving cars or health monitoring systems.

Satellites are another important future source of data. With the growth of commercial space travel and the emergence of relatively cheap nano-satellites, more opportunities are arising for collecting new types of data. This data will increasingly be used for smarter

precision agriculture, in which irrigation and fertilisation could be employed much more precisely. In addition, far more data will become available with regard to various forms and sources of pollution.

Another important future source of data will be our own bodies. Data is becoming more personal and intimate as a result of biometric sensors. Sensors in our body can unlock previously unknown data, with interesting applications in healthcare or possibilities for personalising media. Facial features or drops of sweat can be analysed to predict strokes and hormone levels will be able to reveal underlying problems. This intimate data thus creates new possibilities for self-knowledge, but also raises questions about privacy and freedom.

In a broader sense, the possibility and need to collect ever-more data is at odds with a practical and moral need to minimise the amount of data collected. This can be done by only storing raw data at a higher level of aggregation. For example, a supermarket may retain that a customer is a vegetarian, without necessarily saving all individual purchases. This can also be done by using certain types of sensors that provide sufficient data, without creating an abundance of data that overloads systems and could also be used for untoward purposes. For example, even a relatively simple infrared sensor can monitor human behaviour in, for example, an autonomous car, so it is not necessary to acquire high-quality images for the same purpose.

5. Intelligence

The applications of AI are expanding, and these systems are becoming more creative and will come to operate independently increasingly often. They are also becoming more versatile and more easily tailored to our customs and values.

Artificial intelligence

In recent years, developments in AI have predominantly related to deep learning techniques, methods to build self-learning statistical models based on both labelled and unlabelled data. Major strides have also been made in other forms of machine learning, such as understanding natural language, but only moderate further progress is expected in these approaches.

In the coming years, other AI techniques will gain relevance, such as symbolic and causal machine learning, in which, besides the use of statistics to find patterns and correlations, the learning of causal inferences is "pre-programmed". Furthermore, the domain of evolutionary computation, in which computers arrive at ever-improved solutions through an iterative process of variation and selection, will find more applications in the physical world in the coming years (e.g. in genetic algorithms, robotics).

Based on these types of new AI techniques, low-cost computing power and the availability of more and better data, it is expected that the AI market will see further growth in the coming years. This applies to a number of areas of application in particular:

Computer vision: Computer vision is crucial to all kinds of (semi-)autonomously operating systems, such as delivery drones and self-driving cars, in order for them to move around in our environment and to be able to interact with us and each other. In addition, computer vision offers superhuman possibilities with regard to, for example, molecular level analyses and medical diagnoses.

Natural Language Processing: NLP will continue to improve, until we are able to talk to digital assistants without any problems and frictionless real-time translation from person to person is possible. Language-proficient computers will also enable, for example, care robots to provide more empathetic care and illiterate and visually impaired people to have easier access to digital services.

Cyberwarfare: A cause for concern is that AI will come to play a greater role in a military context and hybrid warfare in the coming years. Consider, for example, our enemies using deepfakes, autonomous weapons, misinformation, and AI systems for purposes of identification, analysis of behaviour and possibly the oppression of groups of people (e.g. the implementation of facial recognition software helps the Chinese state detect and suppress dissidents).

Sustainable AI: The analytical capacity of AI will contribute to sustainability in the coming years by, for instance, optimising industrial and agricultural practices, but also by measuring and analysing the impact of human actions on nature. The latter is challenging, given the many factors that play a role in complex natural systems, and AI can help discover relevant connections.

Emotional AI: Biometric data can analyse real-life human emotions and moods based on body movement, facial expressions, heat or air pressure. Innovations in hardware (e.g. neuromorphic chips) and software (e.g. brain emulation) will further stimulate innovation in this domain. When machines "understand" our emotions and behaviour better, this will lead to better communication with machines and higher added value.

Creative AI: AI could also come to play a greater role in design and creative productions. Generative models can map human creativity based on actions, sentences and images, mimic these processes and possibly initiate their own creative processes. In so-called generative adversarial networks, neural networks help each other to perform better and better by assessing each other's output in an iterative process. Of course, the question remains whether this can be seen as real creativity and whether it is possible to break down the artistic intuition into a series of computational steps, or if it is in fact a uniquely human feature.

Ethics and AI

Now that AI is becoming increasingly prevalent in our daily lives, public and private systems, legislation cannot and will not lag behind. We have come to realise this more keenly over the past five years, prompted by awareness of fake news, filter bubbles, and deepfakes circulating around the time of the U.S. elections, but also of the importance of AI in the geopolitical power struggle between the U.S. and China. As was the case with the internet, and many other technologies in the past, the laws and regulations pertaining to the development and application of AI have been relatively free, and the applications of AI are mainly commercially oriented (despite the fact that a lot of fundamental scientific research is financed by public

In response to this centralisation of power of the providers of services and applications, who are thus enabled to prescribe the rules of use and develop extractive business models based on stored user data, there is a counter-movement of "fat protocols". In these, it is not the applications that reap most of the benefits, but the microservices and applications that work on decentralised protocols. Because user value and data are not owned by the application and service providers but are in shared ownership of the network, on a blockchain, for example, there is an incentive for individual users to contribute to the network through services and innovation.

These incentives can be formalised by way of cryptocurrencies, whose value itself thus becomes a function of the network's value creation. This creates centralisation at the level of the soft infrastructure protocols, but political and economic decentralisation at the level of data and services, thus stimulating the growth of decentralised applications, i.e. dApps. Some large companies are already gearing up for this, such as Facebook's Libra or Microsoft's Identity Overlay Network.

7. Interfaces

The interfaces between us and the underlying Stack are becoming more versatile, more intimate and subtler. The computer is disappearing to the background, giving rise to a more intuitive, more accessible and richer experience.

Had there been no regard for user-friendly interfaces, users would still have to manipulate individual transistors at the most basic level to operate computers. With the power of software and the use of input and output equipment, it is possible to automate, abstract and design these "low-level" interactions in such a way that they become more user-friendly and intuitive forms of interaction. For example, the graphic interface and the computer mouse made it possible to use programs and files through the metaphor of a desktop, eliminating the need for technical computer commands. This means that a user interface is not just the sum of hardware and software, but also comprises the "language" with which people can communicate with computers.

Although many digital systems still use traditional interfaces such as keyboard, mouse and touchscreen, the shift towards more natural interaction metaphors will continue in the coming years. As a result, computers will be able to address an increasingly wide range of users. Because little prior knowledge is required to use computers, we will see the addition of both many younger and older users. Below are a number of modalities that could make up this natural multimodal user interface of the future.

Virtual Reality glasses

Virtual reality glasses visually transport the user to an immersive virtual world through a stereoscopic first-person perspective. The convergence of high-quality yet affordable display technology, sensor technology (gyroscopes, accelerometers, 3D cameras) and processing power has brought VR within reach of the ordinary consumer over the past ten years. In the next ten years, VR glasses are expected to become more and more mainstream due to advances in screen resolution, less image delay and a larger viewing angle. In addition, the glasses will become more compact, more comfortable and cheaper.

Augmented Reality glasses

Instead of being visually locked into a virtual world, it is also possible to project virtual elements over the physical world through augmented reality glasses. Visual elements can simply be placed over the physical world as a floating layer, or they can be placed in "in the room" by means of 3D optical sensors and create the illusion that these objects are present in the physical world.

It is expected that VR will take on the immersive and escapist character of television, while AR is more likely to assume the hermeneutical role of the smartphone. In addition, AR will also be used in professional contexts in which intuition, speed and immersion are required. Think of fighter pilots who need all the relevant information in a fraction of a second, or a police officer who must be able to quickly assess an unsafe situation.

Haptic interfaces

Most interfaces are generally visual and auditory in nature. Nevertheless, computers can also communicate with us through our tactile senses via so-called haptic elements. Consider, for example, your vibrating smartphone, or the shaking of your game console controller. It is expected that virtual reality will gain ground in the future and that these haptic interfaces will be used to increase realism. Examples are haptic suits that allow us to feel virtual touches, the impact of a bullet or even temperature differences.

Interfaces based on gestures

The arrival of every new computing platform was accompanied by a new form of input or way of issuing commands; on the desktop computer this was the mouse, on the smartphone it was the touchscreen. VR and AR will have to have a form of input that offers a similar degree of fine-motor input in the interaction with 3D worlds. With VR, gestures are currently entered through hand controllers. However, as the stylus for general input was not well-suited to the smartphone's dynamic usage context, similarly, AR is not likely to include physical handheld controllers in the future. Instead, finger, hand and arm gestures will be closely tracked by sensors in wearables (bracelets, watches, clothing). This form of input thus offers the most flexibility for the countless contexts in which AR will be used.

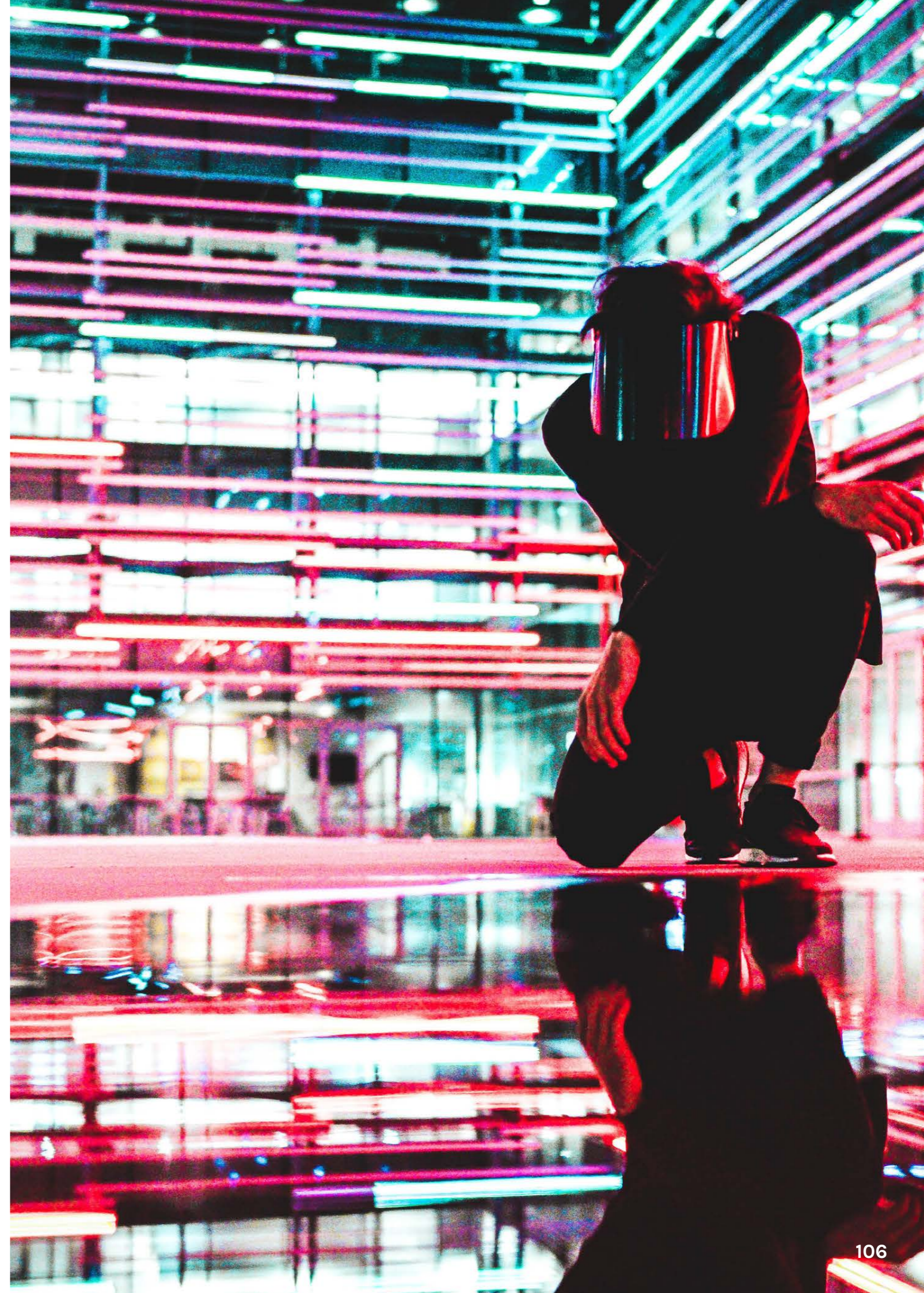
Voice-controlled interfaces

Advances in Natural Language Processing (NLP), voice recognition and speech synthesis in combination with new hardware interfaces such as wireless earphones and smart home systems will further improve the quality of voice-controlled interfaces. In light of further developments within AI, we may expect voice-controlled interfaces to be able to detect emotions and other elements such as physical condition as well as commands. This will allow these virtual assistants to become much more personal and context-sensitive in the future.

Brain Computer Interfaces

The holy grail in human-computer interaction is the development of the brain-computer interface (BCI), with which computers can be operated directly with the brain. Although BCIs were initially developed for brain research and for people with a physical disability, in the future they will also be used to operate everyday applications. With BCIs there are invasive (e.g. neural interface) and non-invasive techniques (e.g. EEG). Although invasive techniques achieve greater bandwidth and precision, for most of them this added value will not outweigh the disadvantages of substantial surgical intervention anytime soon.

An important legal aspect is that employees currently still have to take too much corrective action with automatic systems, but often lack a clear enough overview to do this. In these cases, there is a legal solution, as someone is liable in the event of an error and damage. But this is "instigation", which becomes even more difficult when the insights of AI are not transparent or comprehensible to humans. This certainly applies to policymakers and virtual simulations, because they are in the position of being held accountable for their monitoring function and the execution of any action suggested by AI.



References

¹ Federated Machine Learning is a form of AI in which an algorithm is trained “on location”. That is, the algorithm gets access to a database, and can learn, based on that data, without that data finding its way to the developer of the algorithm and without the possibility to reconstruct the data.

² The Libra consortium has broken up, but Facebook is still working on its own digital currency (Diem).

³ <https://www.fintech.finance/01-news/what-is-programmable-money/>

⁴ <https://ec.europa.eu/trade/policy/in-focus/conflict-minerals-regulation/>

⁵ <https://www.weforum.org/agenda/2021/01/consumer-electronics-managing-e-waste/vlfi>

⁶ <https://www.cbs.nl/nl-nl/maatwerk/2020/51/elektriciteit-geleverd-aan-datacenters-2017-2019#:~:text=In%202017%20kregen%20de%20datacenters,het%20openbaar%20net%20naar%20datacenters.>

⁷ <https://www.nature.com/articles/d41586-018-06610-y>

⁸ <https://royalsocietypublishing.org/doi/abs/10.1098/rsta.2019.0061>

⁹ <https://riscv.org/>

¹⁰ <https://www.nature.com/articles/s41586-019-1666-5>

¹¹ <https://science.sciencemag.org/content/370/6523/1460>

¹² <https://www.sciencemag.org/news/2020/07/biggest-flipping-challenge-quantum-computing>

¹³ <https://www.datacenterknowledge.com/industry-perspectives/how-edge-data-centers-will-save-internet>

¹⁴ <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2019/06/11/nota-mobiele-communicatie/Nota+Mobiele+Communicatie.pdf>

¹⁵ https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17131

¹⁶ <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/connected-world-an-evolution-in-connectivity-beyond-the-5g-revolution>

¹⁷ Different standards are being developed simultaneously for this type of connection, but Wi-Fi and Bluetooth will also continue to play a substantial role in this.

¹⁸ <https://ieeexplore.ieee.org/document/8710704>

¹⁹ <https://www.idc.com/getdoc.jsp?containerId=prUS46286020>

²⁰ <https://www.sciencedirect.com/science/article/pii/S1877050916316957>

Consulted experts

- Prof. dr. Tibor Bosse - Radboud Universiteit
- Dr. Hans Bouwknecht - UNSense
- Prof. dr. José van Dijck – Universiteit Utrecht
- Dr. Yoni van den Eede – Vrije Universiteit Brussel
- Prof.dr.ir. Rinie van Est – Rathenau Instituut
- Prof. dr. Desiree van Gorp - Nyenrode Business Universiteit
- Dr. Pim Haselager – Radboud Universiteit
- Prof. Tom Heskes – Radboud Universiteit
- Dr. Max Hinne – Radboud Universiteit
- Prof.dr.ir. Geert Jan Houben - TU Delft
- Prof. dr. Jeroen van den Hoven - TU Delft
- Chris Huls – Rabobank Tech Lab
- Dr. Dimitri de Jonghe – Co-founder Keyko
- Jonathan Knegtel – Blockdata
- Emmelien Kneppers - UNSense
- Linda Kool – Rathenau
- Simon Lelieveldt – Regulatory and Compliance Consultant
- Dr. Pieter Lemmens - Radboud Universiteit
- Prof. Dr. Derk Loorbach – DRIFT / Erasmus Universiteit Rotterdam
- Douwe Lycklama - Innopay
- Jeroen van Mastrigt – Creatief Strateeg
- Sico van der Meer - Instituut Clingendael
- Prof.dr. Jos de Mul – Eurasmus Universiteit Rotterdam
- Dr. Ir. Melanie Peters – Rathenau Instituut
- Ronald Prins - Hunt & Hackett
- Miriam Rasch - Willem de Kooning Academie
- Dr. Haroon Sheikh - WRR
- Prof. dr. Peter Sloot – Universiteit van Amsterdam
- Prof.dr.ir. Maarten Steinbuch - TU Eindhoven / Scientific Director Eindhoven Engine
- Marleen Stikker - Waag
- Dr. Cor van der Struijf – IBM Quantum Ambassador
- Toon Toetenel - Breaking Bits
- Sander van der Waal - Waag

About FreedomLab

FreedomLab is an independent think tank dedicated to future studies. For over 15 years, it has supported public and private organisations in strategic decision-making. To this aim, FreedomLab develops scenarios at the intersection of geopolitics, technology and culture. Its unique vision and analyses combine insights from philosophy and speculative design with professional knowledge. With its legacy from investment management, FreedomLab is particularly capable of identifying opportunities in times of change.



Sjoerd Bakker

Sjoerd is a senior researcher and strategist. He holds a PhD Innovation Studies from Utrecht University and has authored several peer-reviewed papers on topics including socio-technical transitions and sustainable mobility. In 2017, he published the book *From Luxury to Necessity: what the railways, electricity, and the automobile teach us about the IT revolution*.



Arief Hühn

Arief is head of FreedomLab. He holds a PhD in human-computer interaction from Eindhoven University of Technology. He has published papers on persuasive technology, interface design and simulation-based research methods. Arief is particularly interested in emerging computing platforms (AR/VR, AI, cloud, blockchain, quantum computing) and their impact on society and global power relations.



Sebastiaan Crul

Sebastiaan is a researcher and strategist at FreedomLab. He has a background in philosophy and economics and is currently mainly focused on the future of healthcare, media and entertainment and the digitalisation of everyday life.



Pim Korsten

Pim is a researcher and strategist. He has a background in macro-economics, philosophy of economics and philosophy of history. At FreedomLab, Pim is mostly concerned with changes in the economy in general, geopolitics and international markets. Presently, he is particularly interested in the ways in which new technology can contribute to a more inclusive and sustainable society.

Editor

Petra Berendrecht

Design

Esmee van Dam

Joep Schot

Tessa Steenkamp - Bits of Space

Translation

Lisa Negrijn



**freedom
lab** thinktank for
future scenarios